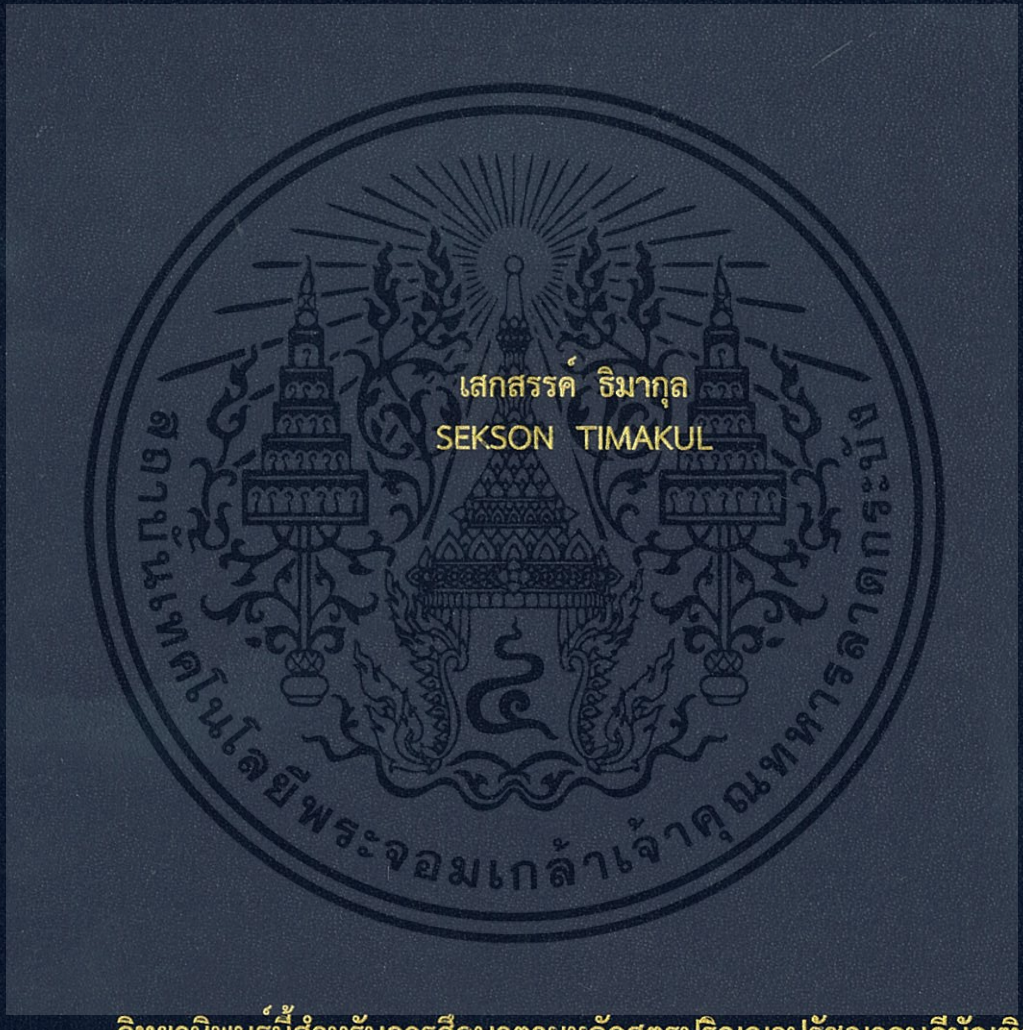
การออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีที่มีเกิรธขนาดใหญ่

DESIGN OF PARITY-CHECK MATRIX FOR LDPC CODES OF LARGE GIRTH



เสกสรรค์ ธิมากุล
SEKSON TIMAKUL

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต
สาขาวิชาเทคโนโลยีการบันทึกข้อมูล
วิทยาลัยนวัตกรรมการผลิตขั้นสูง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2559

KMITL-2016-DS-D-001-01

การออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีที่มีเกิรธขนาดใหญ่

DESIGN OF PARITY-CHECK MATRIX FOR LDPC CODES OF LARGE GIRTH

เสกสรรค์ ธิมากุล
SEKSON TIMAKUL

วิทยานิพนธ์นี้สำหรับการศึกษาตามหลักสูตรปริญญาปรัชญาดุษฎีบัณฑิต
สาขาวิชาเทคโนโลยีการบันทึกข้อมูล
วิทยาลัยนวัตกรรมการผลิตขั้นสูง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
พ.ศ.2559
KMITL-2016-DS-D-001-01

DESIGN OF PARITY-CHECK MATRIX FOR LDPC CODES OF LARGE GIRTH

SEKSON TIMAKUL

A THESIS SUBMITTED IN FULFILLMENT
OF THE REQUIREMENT FOR THE DEGREE OF
DOCTOR OF PHILOSOPHY PROGRAM IN DATA STORAGE TECHNOLOGY
COLLEGE OF ADVANCED MANUFACTURING INNOVATION
KING MONGKUT'S INSTITUTE OF TECHNOLOGY LADKRABANG
2016

KMITL-2016-DS-D-001-01

วิทยาลัยนวัตกรรมการผลิตขั้นสูง
สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
ใบรับรองวิทยานิพนธ์

หัวข้อวิทยานิพนธ์ การออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีที่มีเกิรธขนาดใหญ่
Thesis Title DESIGN OF PARITY-CHECK MATRIX FOR LDPC CODES OF LARGE GIRTH
นักศึกษา นายเสกสรรค์ ธิมากุล
รหัสประจำตัว 52690102
ปริญญา ปรัชญาดุษฎีบัณฑิต
สาขาวิชา เทคโนโลยีการบันทึกข้อมูล
อาจารย์ที่ปรึกษาวิทยานิพนธ์ รศ.ดร.สมศักดิ์ ชุมช่วย
หมายเลขวิทยานิพนธ์ KMITL-2016-DS-D-001-01

คณะกรรมการสอบวิทยานิพนธ์		ลายมือชื่อ
ศาสตราจารย์ ดร.พรชัย	ทรัพย์นิธิ	
รองศาสตราจารย์ ดร.ปิยะ	โควินท์ทวีวัฒน์	
ผู้ช่วยศาสตราจารย์ ดร.จตุพร	ทองศรี	
ผู้ช่วยศาสตราจารย์ ดร.ชานนท์	วริสาร	
รองศาสตราจารย์ ดร.สมศักดิ์	ชุมช่วย	

วัน/เดือน/ปี ที่สอบ 8 เมษายน 2559 เวลา 10.00 - 12.00 น.
สถานที่สอบ อาคารเฉลิมพระเกียรติ 55 พรรษา สมเด็จพระเทพรัตนราชสุดาฯ สยามบรมราชกุมารี

วิทยาลัยนวัตกรรมการผลิตขั้นสูง รับรองแล้ว

(ผู้ช่วยศาสตราจารย์ ดร.ศิริเดช บุญแสง)
คณบดี วิทยาลัยนวัตกรรมการผลิตขั้นสูง

วันที่ 31 **พฤษภาคม พ.ศ.** 2559

หัวข้อวิทยานิพนธ์	การออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีที่มีเกิรธขนาดใหญ่
นักศึกษา	นายเสกสรรค์ ธิมากุล
รหัสประจำตัว	52690102
ปริญญา	ปรัชญาดุษฎีบัณฑิต
สาขาวิชา	เทคโนโลยีการบันทึกข้อมูล
พ.ศ.	2559
อาจารย์ผู้ควบคุมวิทยานิพนธ์	รองศาสตราจารย์ ดร. สมศักดิ์ ชุมช่วย

บทคัดย่อ

รหัสแอลดีพีซีเป็นรหัสควบคุมความผิดพลาดที่มีสมรรถะเข้าใกล้ขอบเขตแชนนอน โดยทั่วไปวิธีการสร้างรหัสแอลดีพีซีสามารถแบ่งเป็น 2 ประเภท คือ แบบสุ่ม และ แบบโครงสร้างที่แน่นอน ทั้ง 2 แบบมีวิธีการสร้างเมทริกซ์ตรวจสอบพาริตี้แยกย่อยออกไปอีกได้หลายแบบ โดยทุกโครงสร้างทั้ง 2 แบบที่ได้กล่าวมาได้รับการออกแบบมุ่งเน้นในการแก้ไขข้อมูลผิดพลาดให้สามารถแก้ไขข้อมูลผิดพลาดให้ได้มากที่สุด วิทยานิพนธ์นี้ได้นำเสนอวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีที่เป็นรูปแบบรหัสควอไซไซคลิค (หรือเรียกว่ารหัสควอไซไซคลิคแอลดีพีซี) ซึ่งเป็นแบบโครงสร้างที่แน่นอน โดยการออกแบบมุ่งเน้นให้เมทริกซ์ตรวจสอบพาริตี้มีค่าเกิรธมากที่สุดเท่าที่จะมากได้ เนื่องจากเกิรธที่มีขนาดใหญ่ขึ้นจะส่งผลให้สมรรถนะของรหัสแอลดีพีซีดียิ่งขึ้น วิธีการออกแบบที่นำเสนอนี้ออกแบบโดยการกำหนดขนาดของเมทริกซ์หมุนสลับตำแหน่งและกำหนดค่าอิลิเมนต์ที่เหมาะสมในการสร้างเมทริกซ์เป็นเลขจำนวนเฉพาะเพื่อสร้างเมทริกซ์แม่โดยให้น้ำหนัก 1 ในแนวตั้งเท่ากับ 3 จากนั้นจึงเลือกเมทริกซ์ย่อยจากเมทริกซ์แม่ในบางหลักมาต่อเรียงกันใหม่อีกครั้งเพื่อสร้างรหัสแอลดีพีซีให้ได้ตามอัตรารหัสที่ต้องการ วิธีที่นำเสนอนี้สามารถออกแบบให้เมทริกซ์ตรวจสอบพาริตี้ให้ได้เกิรธเท่ากับ 6, 8, 10 หรือ 12 และมีสมรรถนะในการแก้ไขข้อมูลผิดพลาดที่ได้ดีกว่าวิธีการออกแบบของแทนเนอร์ โดยที่อัตรารหัส 0.4 และ 0.5 ใช้ค่าสัญญาณต่อสัญญาณรบกวนต่ำกว่าประมาณ 1 เดซิเบลที่อัตราบิตผิดพลาดเท่ากับ 10^{-5} โดยที่จำนวนรอบการถอดรหัสเท่ากับ 20 รอบ

Thesis	Design of parity-check matrix for LDPC codes of large girth
Student	Mr.Sekson Timakul
Student ID.	52690102
Degree	Doctor of Philosophy
Program	Data Storage Technology
Year	2016
Thesis Advisor	Associate Professor Dr. Somsak Choomchuay

ABSTRACT

Low-density parity-check (LDPC) code is an error correcting code with near Shannon limit capability. In general, designing of LDPC code can be divided into two categories: As a result the designed parity-check matrix can be either a random one or a structured one. Both categories can be further divided into several sub-categories. However, all those sub-categories have focused on the feature of as many as possible errors correcting. This thesis proposed a method of parity-check matrix design for LDPC with quasi-cyclic structure (quasi-cyclic LDPC code). The design emphasized on the parity-check matrix that can offer good large girth since the performance of LDPC codes can be increased when the girth is larger. In this method, the size of circulant matrix is a prime number. Elements of the mother matrix are member of such a prime number field. The column weigh is set to 3. From the mother matrix, some sub-matrices are selected and concatenated to form a new parity-check matrix for any code rate. With this proposed method, parity-check matrix can offer the girth of 6, 8, 10 and 12. The performance of the resulted code is better than that of the Tanner's designs. At the code rate of 0.4 and 0.5, and 20 iteration runs, the gain of 1dB, at the BER of 10^{-5} can be achieved.

กิตติกรรมประกาศ

ในการวิจัยครั้งนี้ผู้วิจัยขอขอบพระคุณ รศ.ดร.สมศักดิ์ ชุมช่วย ซึ่งเป็นอาจารย์ที่ปรึกษาและผู้ควบคุมวิทยานิพนธ์ที่กรุณาให้คำปรึกษาแนะนำเกี่ยวกับการทำวิจัยนี้จนสำเร็จลุล่วงไปได้ด้วยดี

ขอขอบคุณศูนย์เทคโนโลยีอิเล็กทรอนิกส์และคอมพิวเตอร์แห่งชาติ สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ ที่สนับสนุนทุนการศึกษาระดับปริญาเอกและในงานวิจัยแก่ข้าพเจ้า

สุดท้ายนี้ขอขอบพระคุณ บิดา-มารดา ครู-อาจารย์ และครอบครัวของข้าพเจ้าที่สนับสนุนและเป็นกำลังใจให้ข้าพเจ้ามาโดยตลอด

คุณค่าและประโยชน์อันพึงมีที่เกิดจากงานวิจัยนี้ ข้าพเจ้าขอมอบแด่ผู้มีพระคุณทุกท่าน

เสกสรรค์ ธิมากุล

สารบัญ

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญ (ต่อ)

หน้า

สารบัญตาราง

สารบัญรูป

บทที่ 1
บทนำ

บทนี้จะกล่าวถึงความเป็นมาและความสำคัญของปัญหาที่มาของการทำงานวิจัยครั้งนี้รวมถึงบอกวัตถุประสงค์ สมมุติฐาน ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย ขอบเขต และขั้นตอนการวิจัย โดยมีรายละเอียดดังต่อไปนี้

1.1 ความเป็นมาและความสำคัญของปัญหา

ในปัจจุบันการสื่อสารระบบดิจิทัลได้ถูกนำมาใช้อย่างแพร่หลาย เช่น โทรศัพท์มือถือ โทรทัศน์ระบบดิจิทัลผ่านดาวเทียมหรือเคเบิล ระบบอินเตอร์เนตไร้สายต่อผ่าน Wi-Fi หรือ Wi-Max และระบบอินเตอร์เนตต่อผ่านโมเด็ม นอกจากนี้ยังถูกนำไปใช้ในอุปกรณ์จัดเก็บข้อมูลดิจิทัล เช่น ฮาร์ดดิสก์ไดรฟ์ (Hard Disk Drive), ออฟติคอลดิสก์ไดรฟ์ (Optical Disk Drive เช่น CD, DVD และ Blu-ray) และ แฟลชไดรฟ์ (Flash Drive) ซึ่งในการส่งข้อมูลเชิงดิจิทัลผ่านช่องสื่อสารแบบต่าง ๆ หรือระบบการจัดเก็บข้อมูลหลีกเลี่ยงไม่ได้ที่จะพบปัญหาคุณภาพของสัญญาณที่รับได้ที่ภาครับหรือการอ่านข้อมูลที่จัดเก็บ โดยมีสาเหตุหลายประการ เช่น สัญญาณรบกวนที่เกิดขึ้นภายในช่องสื่อสาร และสัญญาณรบกวนจากภายนอกหรือคุณลักษณะที่ไม่อุดมคติของช่องสัญญาณ จากประเด็นปัญหาดังกล่าวเหล่านี้ Shannon [1] ได้ค้นพบทฤษฎีการส่งข้อมูลผ่านช่องสื่อสารในปี ค.ศ 1948 โดยแสดงให้เห็นว่า ข้อมูลดิจิทัลสามารถถูกส่งผ่านช่องสื่อสารได้อย่างมีประสิทธิภาพและมีความผิดพลาดน้อยมากถ้าอัตราการส่งข้อมูล (Data Rate) ไม่เกินความจุของช่องสื่อสาร (Channel Capacity) และมีการเข้ารหัสข้อมูลที่ต้นทาง (Data Encoding) จากนั้นก็มีการถอดรหัสข้อมูลที่ปลายทาง (Data Decoding) ที่เหมาะสม จากนั้นมานักวิจัยทั่วโลกก็ได้คิดค้นเทคนิคต่าง ๆ มาอย่างต่อเนื่องเพื่อที่จะให้ได้ประสิทธิภาพของการส่งข้อมูลสูงสุดตามทฤษฎีดังกล่าว ปัจจุบันความต้องการของผู้ใช้บริการระบบสื่อสารหรือการจัดเก็บข้อมูลดิจิทัลมีความต้องการเพิ่มขึ้นมากเรื่อยๆ ไม่ว่าจะเป็นความเร็วของการส่งข้อมูล ประสิทธิภาพของข้อมูลที่รับได้จะต้องมีความถูกต้อง ขนาดข้อมูลที่มีขนาดใหญ่ เทคนิคหนึ่งที่มีบทบาทมากในระบบสื่อสารเพื่อตอบสนองต่อความต้องการต่าง ๆ เหล่านี้คือเทคนิคการเข้ารหัสเพื่อแก้ไขความผิดพลาดล่วงหน้า (Forward Error Correction, FEC)

โดยรหัสควบคุมความผิดพลาด (Error Control Codes, ECC) เป็นแขนงหนึ่งในการประมวลสัญญาณ ที่ใช้อย่างแพร่หลายในการสื่อสารสมัยใหม่ การกระทำเป็นการอนุมานว่าความผิดพลาดจะเกิดขึ้นอย่างแน่นอน และมีการเตรียมพร้อมที่จะแก้ไขความผิดพลาดนั้น ซึ่งเป็นหนึ่งในเทคนิคของวิธีการแก้ไขความผิดพลาดไว้ล่วงหน้า รหัสควบคุมความผิดพลาดนั้น แบ่งเป็น 2 แบบ คือ แบบที่ตรวจสอบได้ว่า เกิดความผิดพลาดขึ้น (Error Detection) และแบบที่แก้ไขความผิดพลาดได้ด้วย (Error Correction)

- Error Detection Code ที่ใช้กัน แพร่หลาย คือ Parity Check Code และ Cyclic Redundant Code (CRC)
- Error Correction Code มีใช้กันแพร่หลาย 2 กลุ่ม คือ กลุ่มรหัสบล็อก (Block Code) เช่น รหัสแฮมมิง, รหัสบีซีเอช, รหัสรีด-โซโลมอน และรหัสแอลดีพีซี ในกลุ่มรหัสคอนโวลูชั่น (Convolutional Code) เช่น รหัสคอนโวลูชั่น และรหัสเทอร์โบ

เนื่องจากรหัสแอลดีพีซีมีประสิทธิภาพในการแก้ไขข้อผิดพลาดได้ดีและเป็นรหัสที่มีประสิทธิภาพเข้าใกล้ขอบเขตของแชนนอนเทียบเท่ารหัสที่มีประสิทธิภาพสูงอย่างรหัสเทอร์โบ แต่มีความซับซ้อนน้อยกว่ารวมทั้งรหัสแอลดีพีซีไม่มีสิทธิบัตรคุ้มครองสามารถนำพัฒนาและผลิตโดยไม่เสียค่าใช้สิทธิแต่อย่างใด ทำให้นักวิจัยต่างสนใจกันอย่างมากโดยการวิจัยจะมุ่งเน้นไปที่การวิเคราะห์และปรับปรุงรหัสแอลดีพีซีให้ดีขึ้น ซึ่งปัจจุบันรหัสแอลดีพีซีได้รับการนำเสนอไปใช้ร่วมกับระบบต่าง ๆ มากมายในปัจจุบันเช่น นำไปใช้ร่วมกับระบบการสื่อสารไร้สาย ระบบการสื่อสารดาวเทียมและระบบฮาร์ดดิสก์ไดรฟ์

จากที่ได้กล่าวมาแล้วข้างต้นถึงการนำรหัสแอลดีพีซีมาใช้ในปัจจุบัน โดยนักวิจัยจำนวนมากได้คิดค้นวิธีการออกแบบรหัสแอลดีพีซีโดยมุ่งเน้นไปที่การออกแบบเมทริกซ์ตรวจสอบพาริตี้ ซึ่งประกอบด้วยโครงสร้างใหญ่ๆ 2 แบบ คือ แบบสุ่ม และ แบบโครงสร้างที่แน่นอน โดยแต่ละแบบจะมีวิธีการต่าง ๆ แยกย่อยอีกมากมาย ซึ่งวิธีการแต่ละแบบมุ่งเน้นในการแก้ไขข้อมูลผิดพลาดให้แก้ไขข้อมูลผิดพลาดให้มากที่สุด แต่ทั้งนี้วิธีการออกแบบตรวจสอบพาริตี้บางวิธีที่ทำให้รหัสแอลดีพีซีได้ประสิทธิภาพที่ดีนั้นอาจไม่เหมาะสมในการนำไปประยุกต์ใช้โดยการสร้างเป็นฮาร์ดแวร์ เนื่องจากมีความซับซ้อนสูง เช่น แบบสุ่ม ส่วนโครงสร้างแบบคงที่แม้ว่าจะเหมาะสมมากกว่าแบบสุ่มในเชิงฮาร์ดแวร์แต่ประสิทธิภาพในการแก้ไขข้อมูลผิดพลาดนั้นด้อยกว่าหรือบางวิธีมีข้อจำกัดต่ออัตรารหัสค่าต่าง ๆ จากปัญหาดังกล่าวนี้เป็นแรงจูงใจผู้วิจัยต้องการที่ทำการออกแบบรหัสแอลดีพีซีที่มีประสิทธิภาพสูงและเหมาะสมในการสร้างเชิงฮาร์ดแวร์ โดยผู้วิจัยมุ่งเน้นไปที่รหัสแอลดีพีซีที่มีโครงสร้างที่แน่นอนและการออกแบบทำได้โดยง่ายรวมทั้งเหมาะสมในการนำไปประยุกต์ใช้งานจริงทั้งในระบบสื่อสารดิจิทัลหรือระบบจัดเก็บข้อมูล

1.2 ความมุ่งหมายและวัตถุประสงค์ของการศึกษา

วิทยานิพนธ์ฉบับนี้มุ่งเน้นการศึกษาและพัฒนารหัสแอลดีพีซีให้มีประสิทธิภาพดียิ่งขึ้นจากโครงสร้างรหัสแอลดีพีซีแบบควอไซไซคลิคที่มีขนาดเกิรธ (Girth) ที่มีขนาดเท่ากับหรือมากกว่า 6 โดยการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่มีโครงสร้างที่แน่นอนและเหมาะสมในการนำไปประยุกต์ใช้งานจริงด้วยการสร้างเป็นฮาร์ดแวร์ นอกจากนี้การออกแบบดังกล่าวจะเปรียบเทียบสมรรถนะกับโครงสร้างรหัสแอลดีพีซีแบบต่าง ๆ

1.3 สมมุติฐานของการศึกษา

เมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซีโดยใช้โครงสร้างของรหัสควอไซไซคิคภายใต้ระบบสัญญาณรบกวนแบบเกาส์เซียนที่มีสมรรถนะที่ดีเทียบเท่าหรือเหนือกว่าการออกแบบด้วยวิธีการเมทริกซ์ตรวจสอบพาริตี้ด้วยวิธีการต่าง ๆ ในปัจจุบัน ทั้งโครงสร้างแบบสุ่ม และ โครงสร้างที่แน่นอน โดยการออกแบบเพื่อกำจัดลูป 4 และลูป 6 เพื่อทำให้เกิรธมีขนาดเท่ากับหรือมากกว่า 8 ตั้งแต่อัตรารหัสที่ต่ำจนถึงอัตรารหัสที่สูง

1.4 ทฤษฎีหรือแนวความคิดที่ใช้ในการวิจัย

ทฤษฎีที่ใช้ในการออกแบบจะใช้กลุ่มผลคูณของการมอดูโล (Modulo) เลขจำนวนเต็ม p ในการสร้างเมทริกซ์พาริตี้แม่ (Mother H matrix) บนโครงสร้างควอไซไซคลิค โดยสร้างจากอิลิเมนต์ที่สามารถสร้างสมาชิกได้ครบทุกค่า และแนวคิดที่จะทำให้เมทริกซ์พาริตี้ใหม่ซึ่งปราศจากลูป 4 และลูป 6 ทำให้เกิรธมีขนาดเท่ากับหรือมากกว่า 8 นั้นมาจากการเลือกหลัก (Column) บางส่วนมาต่อกัน โดยมีแนวทาง 2 แบบ คือ คิดค้นรูปที่แน่นอนในการเลือกหลักมาต่อกัน และอีกวิธีหนึ่งคือเสนออัลกอริทึมในการค้นหาตำแหน่งในการเลือกหลักที่เหมาะสม ในการออกแบบที่นำเสนอนี้สามารถออกแบบให้ได้ขนาดของเกิรธขนาดใหญ่สำหรับน้ำหนัก 1 ในแนวตั้ง (Column weigth) เท่ากับ 3 โดยสามารถออกแบบเพื่อให้ได้ขนาดเกิรธสูงสุดที่ได้มีขนาดเกิรธเท่ากับ 12

1.5 ขอบเขตการวิจัย

งานวิจัยนี้จะทำการศึกษาและออกแบบรหัสความหนาแน่นพาริตี้ต่ำโดยมุ่งเน้นที่รหัสแอลดีพีซีบนโครงสร้างควอไซไซคลิค (Quasi cyclic) โดยกำหนดค่าเมทริกซ์หมุนสลับตำแหน่ง (Circulant Matrix LDPC) และทำวัดประสิทธิภาพโดยการจำลองการทำงานบนช่องสัญญาณรบกวนเกาส์เซียน (AWGN Channel) และทำการเปรียบเทียบกับวิธีการออกแบบรหัสแอลดีพีซีแบบอื่นที่ได้รับความนิยมในปัจจุบัน

1.6 ขั้นตอนของการศึกษา

- ศึกษาเกี่ยวกับรหัสแบบต่าง ๆ ที่ใช้ในการเข้าและถอดรหัส
- ศึกษาคณิตศาสตร์พื้นฐานสำหรับทำความเข้าใจเรื่องรหัสแก้ไขข้อผิดพลาด
- ศึกษาการออกแบบรหัสแอลดีพีซีแบบต่าง ๆ
- ออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซี
- ทดสอบสมรรถนะรหัสแอลดีพีซีตามเมทริกซ์ตรวจสอบพาริตี้ที่ได้ออกแบบภายใต้ระบบสัญญาณรบกวนเกาส์เซียน
- เปรียบเทียบสมรรถนะรหัสแอลดีพีซีที่ออกแบบกับวิธีการออกแบบอื่นๆ
- สรุปและวิจารณ์ผลที่ได้

วิทยานิพนธ์ฉบับนี้ประกอบด้วยบทต่าง ๆ 5 บท บทที่ 1 คือบทนำได้กล่าวถึงความสำคัญและวัตถุประสงค์ของวิทยานิพนธ์ฉบับนี้ บทที่ 2 กล่าวถึงพื้นฐานคณิตศาสตร์, ระบบสื่อสารเบื้องต้นและพื้นฐานรหัสบล็อก บทที่ 3 กล่าวถึงรหัสแอลดีพีซีโดยเน้นถึงโครงสร้างและวิธีการออกแบบต่าง ๆ ประกอบด้วย รหัสอาเรย์, รหัสอาร์เรย์แบบปรับปรุง, รหัสควอไซไซคลิค, รหัสเรขาคณิตยูคลิด, รหัสเรขาคณิตเชิงภาพฉาย, รหัสบล็อกไม่สมบูรณ์แบบสมดุล และอัลกอริทึมพีอีจี พร้อมทั้งตัวอย่างวิธีการออกแบบ และกล่าวถึงการเข้ารหัสและถอดรหัสแบบไบนารี บทที่ 4 กล่าวถึงวิธีการออกแบบรหัสแอลดีพีซีเพื่อให้ได้เกิรธขนาดใหญ่พร้อมตัวอย่างการออกแบบและผลการทดสอบเปรียบเทียบวิธีการออกแบบที่ได้นำเสนอนี้กับวิธีการออกแบบอื่นๆที่ได้กล่าวไว้ในบทที่ 3 โดยทดสอบบนช่องสัญญาณเกาส์เซียนที่อัตรารหัสค่าต่าง ๆ ในการทดสอบจะเปรียบเทียบโครงสร้างที่ออกแบบแต่ละแบบที่มีเกิรธเท่ากับ 6 และโครงสร้างที่สร้างเกิรธได้มากกว่า 6 เปรียบเทียบสมรรถนะกับโครงสร้างที่นำเสนอในวิทยานิพนธ์นี้ และบทสุดท้าย คือ บทที่ 5 เป็นการสรุปผลการวิจัยและข้อเสนอแนะ

บทที่ 2
ทฤษฎีพื้นฐาน

ในบทนี้จะกล่าวถึงคณิตศาสตร์ที่จำเป็นในการในไปใช้ในการออกแบบรหัสแก้ไขข้อมูลผิดพลาดและพื้นฐานของรหัสบล็อก การเข้ารหัสและถอดรหัส และโครงสร้างพื้นฐานของรหัสบล็อกที่จำเป็น ซึ่งทฤษฎีพื้นฐานทั้งหมดในบทนี้จะเป็นพื้นฐานในการออกแบบรหัสแอลดีพีซีในบทถัดไป

2.1 เซตและคณิตศาสตร์ของตัวเลขไบนารี

เซต คือ คณิตศาสตร์ที่ใช้บ่งบอกถึงกลุ่มของสิ่งต่าง ๆ และเมื่อกล่าวถึงกลุ่มใดแน่นอนว่าสิ่งใดอยู่ในกลุ่ม สิ่งใดไม่อยู่ในกลุ่ม ตัวอย่างของเซต $X = \{x_1, x_2, x_3, x_4, x_5\}$ โดยมีองค์ประกอบคือ x_1, x_2, x_3, x_4, x_5 และให้เซตคือ S และตัวเลขในเซต S คือองค์ประกอบของเลขจำนวนจำกัด เรียกว่าเซตจำกัด (Finite set) หรือเซตที่สามารถระบุจำนวนสมาชิกในเซตได้ โดยเซตจำกัดจะใช้ในทฤษฎีของรหัสควบคุมความผิดพลาด จำนวนองค์ประกอบของเซต S เรียกว่า $|S|$ สัญลกษณ์และความหมายของเซตที่สำคัญมีดังนี้

$\varnothing$ เรียกว่าเซตว่าง คือ คือ เซตที่ไม่มีสมาชิกเลย

$X \cup Y$ เรียกว่ายูเนียนของเซต X และ Y คือเซตที่ประกอบด้วยสมาชิกของเซต X หรือ Y หรือทั้งสองเซต

$X \cap Y$ เรียกว่าอินเตอร์เซคชันของเซต X และ Y คือเซตที่ประกอบด้วยสมาชิกของเซต X และ Y

$X \setminus Y$ เรียกว่าผลต่างของเซตของเซต X และ Y คือเซตที่ประกอบด้วยสมาชิกของเซต X แต่ไม่เป็นสมาชิกของเซต Y

คณิตศาสตร์ของตัวเลขไบนารี คือ คณิตศาสตร์ที่มีคุณสมบัติการบวกลบคูณหารด้วยการมอดูโลด้วย 2 โดยมีตัวเลขในการใช้งานเพียง 2 ค่า คือ 0 และ 1 ซึ่งเป็นตัวเลขที่ใช้ในระบบดิจิทัลหรือเลขฐานสอง โดยการบวกและลบกระทำเหมือนการใช้เอ็กซ์คลูซิฟออร์ (XOR) ส่วนการคูณและการหารจะใช้พหุนาม (Polynomial)

2.2 กรุ๊ปจำกัด

กรุ๊ปจำกัด (Finite Groups) คือ กลุ่มในคณิตศาสตร์ขอบเขตจำกัดเป็นเซตที่ประกอบด้วยอิลิเมนท์ (Elements) หรืออ็อบเจกต์ (Objects) กลุ่มคืออ็อบเจกต์ทางคณิตศาสตร์ที่สามารถจะบวกและลบกันได้ โดยคุณสมบัติของกลุ่มมีดังนี้

- ส่วนปิดคลุม (Closure) สำหรับ a และ b ที่อยู่ในเซต $c = a * b$ ก็จะอยู่ในเซตด้วย
- การเปลี่ยนหมู่ (Associativity) สำหรับ a, b และ c ที่อยู่ในเซต $a*(b*c) = (a*b)*c$
- เอกลักษณ์ (Identity) เมื่อ e เป็นอิลิเมนต์เอกลักษณ์ $a*e = e*a = a$
- ส่วนผกผัน (Inverse) เมื่อ a เป็นอิลิเมนต์ในเซต จะมีอิลิเมนต์ผกผันของ a ซึ่ง $a*a' = a'*a = e$

2.3 วงล้อจำกัด

วงล้อจำกัด (Finite Rings) คืออ็อบเจกต์ทางคณิตศาสตร์ที่สามารถบวก ลบ และคูณกันได้ โดยคุณสมบัติของวงล้อมีดังนี้

- R เป็นอาบีเลียนกรุ๊ป (Abelian group) ภายใต้การบวก (+)
- ส่วนปิดคลุม (Closure) สำหรับ a และ b ที่อยู่ในเซต R ค่าของ $c = a * b$ ก็จะอยู่ในเซตด้วย
- กฎการเปลี่ยนหมู่ (Associativity law) สำหรับ a, b และ c ที่อยู่ในเซต $a*(b*c) = (a*b)*c$
- กฎการแจกแจง (Distributive law)
  - $a(b+c) = ab + ac$
  - $(b+c)a = ba + ca$

ในวงล้อจำกัดสามารถแบ่งได้เป็น 2 แบบด้วยกัน คือ วงล้อเลขจำนวนเต็มและวงล้อพหุนาม

2.3.1 วงล้อเลขจำนวนเต็ม

วงล้อเลขจำนวนเต็ม (Integer Ring) คือ เซตของจำนวนเต็ม (จำนวนบวก จำนวนลบ และศูนย์) ที่มีคุณสมบัติตามการกระทำของวงล้อคือ การบวกและการคูณ โดยใช้สัญญลักษณ์ $\mathbb{Z}$

- ในวงล้อ $\mathbb{Z}$ จำนวนเต็ม s หารลงตัวด้วยจำนวนเต็ม r จะได้ $s = ar$ เมื่อ a คือจำนวนเต็มอีกจำนวนหนึ่ง
- ในวงล้อ $\mathbb{Z}$ หากจำนวนเต็ม p สามารถหารลงตัวด้วยตนเองหรือ ± 1 จะเรียกจำนวน p นั้นว่าจำนวนปฐม (Prime integer)
- จำนวนเต็ม ที่ไม่ใช่จำนวนปฐม ก็จะเรียกว่าจำนวนประกอบ (Composite)
- ตัวหารร่วมมาก (Greatest Common Divisor, GCD) ของจำนวนเต็ม 2 จำนวน $GCD(r,s)$ ก็คือจำนวนเต็มที่มีค่ามากที่สุดที่สามารถหาร r และ s ได้ลงตัว
- ตัวคูณร่วมน้อย (Least Common Multiplier, LCM) ของจำนวนเต็ม 2 จำนวน $LCM(r,s)$ คือจำนวนเต็มที่มีค่าน้อยที่สุดที่ทั้ง r และ s หารจำนวนนั้น ได้ลงตัว
- ทั้งจำนวนเต็ม r และ s ถือว่าเป็นจำนวนปฐมสัมพันธ์ (Relative prime) เมื่อ $GCD(r,s) = 1$
- ปกติแล้วในกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p จะไม่นับการหาร แต่อย่างไรก็ตามก็อนุโลมการหารเหลือเศษ

2.3.2 วงล้อพหุนาม

วงล้อพหุนาม (Polynomial Ring) สำหรับจำนวนเต็มบวก q พหุนามบนสนาม $GF(q)$ สามารถเขียนได้โดยสมการคณิตศาสตร์คือ

$$f(x) = a_{n-1}x^{n-1} + a_{n-2}x^{n-2} + \cdots ..... + a_2x^2 + a_1x + a_0$$

โดยที่สัมประสิทธิ์ $a_{n-1}, a_{n-2}, ..., a_2, a_1, a_0$ เป็นสมาชิกใน $GF(q)$

- พหุนามมอนิก (Monic polynomial) ก็คือพหุนามที่ $f_{n-1} = 1$ และพหุนามสองพหุนามจะเท่ากันเมื่อสัมประสิทธิ์ a_i ของแต่ละพหุนามมีค่าเท่ากันสำหรับทุก ๆ ค่าของ i
- ดีกรีของพหุนาม (ใช้ว่า $\deg f(x)$) ก็คือ $n-1$
- เซตของพหุนามใน $GF(q)$ สามารถที่จะต่อกันเป็นวงล้อได้หาก การคูณและการบวกนั้นนิยามเช่นเดียวกับพหุนามปกติ โดยใช้ $GF(q)$ แทนวงล้อของพหุนาม
- การบวกกันของสองพหุนาม $f(x)$ และ $g(x)$ ทำให้ได้พหุนามใหม่ ซึ่ง $f(x) + g(x) = \sum_{i}^{\infty}(f_i + g_i)x^i$ โดยที่ดีกรีสูงสุดของผลลัพท์จะเท่ากับดีกรีของพหุนามเดิม
- การคูณกันของสองพหุนาม $f(x)$ และ $g(x)$ ทำให้ได้พหุนามใหม่ ซึ่งทำได้คือ $f(x)\cdot g(x) = \sum_{i=0}^{i=\infty}\left(\sum_{j=0}^{i} f_i \cdot g_i\right)x^i$ โดยที่ดีกรีสูงสุดของผลลัพท์จะเท่ากับดีกรีของสองพหุนามเดิมบวกกัน
- วงล้อของพหุนามนี้จะมีคุณสมบัติทำนองเดียวกันวงล้อของจำนวนเต็ม

2.4 ฟิลด์จำกัด

ฟิลด์จำกัด (Finite Fields) คือ กลุ่มของอิลิเมนต์ที่มีการกำหนดโอเปอร์เรชันระหว่างอิลิเมนต์ 2 แบบ คือ การบวก (หรือการลบ) และ การคูณ (หรือการหาร) ในกาลัวส์ฟิลด์ โดยกาลัวส์ฟิลด์ (Galois Field) คือ เซตที่มีจำนวนสมาชิกจำกัดและมีคุณสมบัติของความเป็นฟิลด์ โดยใช้สัญลักษณ์ $GF(q)$ แทนฟิลด์ที่มีอันดับเท่ากับ q กาลัวส์ฟิลด์แบบง่ายที่สุดคือ $GF(2^m)$ เมื่อ m คือเลขจำนวนเต็มใด ๆ และเมื่อ $m>1$ จะเรียกเป็นฟิลด์อันดับสูง (high order field) โดยที่สัมประสิทธิ์ของพหุนามจะเป็นสมาชิกของเซตที่มี $q-1$ ค่า คือ $\{0,1,2,..,q-1\}$ โดยมีโอเปอร์เรชันการบวกและการคูณในแบบเลขฐานสอง ใน $GF(q)$ การคำนวณของกาลัวส์ฟิลด์ใช้การบวกพหุนามและการคูณพหุนาม ซึ่งกระทำได้ดังนี้

2.4.1 การบวกพหุนาม

การบวกพหุนาม (Addition of Polynomial) คือ การนำสัมประสิทธิ์ของ พหนุนามที่มีค่ายกกำลังที่เท่ากันมาบวกกัน โดยการบวกจะบวกแบบ XOR ในเลขฐานสอง (ใช้สัญญลักษณ์ $\oplus$) กล่าวคือค่าสัมประสิทธิ์ที่เท่ากันบวกกันจะเป็นศูนย์ ตัวอย่างเช่น

ให้ $a(x)=1+x+x^2$ และ $b(x)=1+x+x^2+x^3+x^4$

$$\begin{aligned} a(x)+b(x) &= (1+x+x^2)+(1+x+x^2+x^3+x^4) \\ &= (1\oplus 1)+(1\oplus 1)x+(1\oplus 1)x^2+(0\oplus 1)x^3+(0\oplus 1)x^4 \\ &= x^3+x^4 \end{aligned}$$

2.4.2 การคูณพหุนาม

การคูณพหุนาม (Multiplication of Polynomial) ในกาลัวส์ฟิลด์เหมือนการคูณเลขจำนวนเต็มแต่จะอยู่ในรูปของกาลัวส์ฟิลด์ และใช้การบวกพหุนามร่วมด้วยในการคำนวณ ตัวอย่างเช่น ให้ $a(x)=1+x+x^2$ และ $b(x)=1+x^3$ โดยใช้พหุนามตั้งต้น $1+X+X^4$ จากพหุนามจะได้ $x^4=1+x$

$$\begin{aligned} a(x)+b(x) &= (1+x+x^2)\times(1+x^3) \\ &= (1+x+x^2)+(x^3+x^4+x^5) \\ &= (1+x+x^2)+(x^3+(1+x)+(x+x^2)) \\ &= (1\oplus 1)+(1\oplus 1\oplus 1)x+(1\oplus 1)x^2+(0\oplus 1)x^3 \\ &= x+x^3 \end{aligned}$$

นอกเหนือจากการบวกพหุนามและคูณพหุนามแล้ว วิธีหนึ่งที่สามารถคำนวณได้อย่างรวดเร็วคืออาศัยตารางการบวกและการคูณ ในการสร้างตารางบวกและตารางคูณทำได้โดยการกำหนดพหุนามที่ใช้และกำหนดค่าเวกเตอร์ ตัวอย่างเช่นตารางที่ 2.1 แสดงตัวอย่างค่าต่าง ๆ ของ $GF(2^3)$ โดยใช้พหุนามตั้งต้น $1+X+X^3$

ตารางที่ 2.1 ค่าต่าง ๆ ของ $GF(2^3)$ โดยใช้พหุนามตั้งต้น $1+X+X^3$

i	α^i	พหุนาม	เวกเตอร์หรือเลขฐานสอง	เลขฐานแปด
$-\infty$	0	0	0 0 0	0
0	1	1	1 0 0	1
1	α	α	0 1 0	2
2	α^2	α^2	0 0 1	4
3	α^3	$1+\alpha$	1 1 0	3
4	α^4	$\alpha+\alpha^2$	0 1 1	6
5	α^5	$1+\alpha+\alpha^2$	1 1 1	7
6	α^6	$1+\alpha^2$	1 0 1	5

จากตารางที่ 2.1 สามารถสร้างตารางการบวกและตารางการคูณได้ดังตารางที่ 2.2 โดยใช้หลักการบวกพหุนามและการคูณพหุนาม

ตารางที่ 2.2 การบวกและตารางการคูณของ $GF(8)$ แสดงในรูปของเลขฐานแปด

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	0	3	2	5	4	7	6
2	2	3	0	1	6	7	4	5
3	3	2	1	0	7	6	5	4
4	4	5	6	7	0	1	2	3
5	5	4	7	6	1	0	3	2
6	6	7	4	5	2	3	0	1
7	7	6	5	4	3	2	1	0

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	3	1	7	5
3	0	3	6	5	7	4	1	2
4	0	4	3	7	6	2	5	1
5	0	5	1	4	2	7	3	6
6	0	6	7	1	5	3	2	4
7	0	7	5	2	1	6	4	3

2.5 ปริภูมิเวกเตอร์

ปริภูมิเวกเตอร์ หรือ เวกเตอร์สเปซ (Vector space) กำหนดให้ V เป็นเซตของอิลิเมนต์ที่เรียกว่า เวกเตอร์ (Vector) และ F เป็นฟิลด์ของอิลิเมนต์ที่เรียกว่า สเกลาร์ (Scalar) ปริภูมิเวกเตอร์มีคุณสมบัติดังนี้

- เวกเตอร์ เป็นกรุ๊ปที่มีคุณสมบัติการสลับที่ (Commutative) ภายใต้โอเปอร์ชั่นการบวก
- สำหรับทุกๆอิลิเมนต์ $a \in F$ และ $v \in V$ ผลการคูณ $a \cdot v \in V$
- สำหรับทุกๆอิลิเมนต์ $a, b \in F$ และ $v \in V$ มีคุณสมบัติการจัดหมู่ (Associativity) เป็น $(a \cdot b) \cdot v = a \cdot (b \cdot v)$
- สำหรับทุกๆอิลิเมนต์ $a, b \in F$ และ $u, v \in V$ มีคุณสมบัติการแจกแจง (Distributivity) เป็น $a \cdot (u + v) = a \cdot u + a \cdot v$ และ $(a + b) \cdot v = a \cdot v + b \cdot v$
- ถ้า "1" เป็นยูนิตอิลิเมนต์ (Unit element) $\in F$ สำหรับทุกๆอิลิเมนต์ $v \in V, 1 \cdot v = v$

2.6 เรขาคณิตจำกัด

เรขาคณิตจำกัด (Finite Geomety) เป็นคณิตศาสตร์ขอบเขตจำกัดที่เกี่ยวกับ จุด (Point), เส้น (Line) และพื้นระนาบ (Flats) และมีนิยามที่เกี่ยวข้องกับการออกแบบรหัสแอลดีพีซีดังนี้

(1) เมื่อจุดสองจุดเชื่อมต่อกันจะได้เส้น 1 เส้น

(2) เส้น 2 เส้นที่ไม่ได้เชื่อมต่อกันจะไม่มีจุดเชื่อมต่อ หรือ เส้น 2 เส้นที่ตัดผ่านกันจะมีจุดเชื่อมต่อ 1 จุด

(3) ถ้าเส้นสองเส้นมีจุดเชื่อมต่อ 2 จุดร่วมกัน เส้นๆนั้นคือเส้นเดียวกัน

เรขาคณิตจำกัดถูกใช้สำหรับการออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซี ซึ่งมีอยู่ 2 รูปแบบคือ เรขาคณิตยูคลิด (Euclid Geomety) และเรขาคณิตเชิงฉายภาพ (Projective Geomety) ซึ่งจะอธิบายการออกแบบเมทริกซ์ตรวจสอบพาริตี้ต่อไปในบทที่ 3

2.6.1 เรขาคณิตยูคลิด

เรขาคณิตยูคลิด (Euclid Geomety) กำหนดให้ค่า m เป็นเลขจำนวนเต็มบวกมีค่ามากกว่า $GF(q)$ เมื่อ q คือค่า p^s และ $s \geq 1$ จะได้มิติ m ของเรขาคณิตยูคลิดสามารถเขียนได้เป็น $EG(m,q)$ ประกอบด้วย จุด, เส้น และระนาบ โดยแต่ละจุดเป็น m-tuple บน $GF(q)$ ดังนั้นจุดที่บน $GF(q)$ มาจากปริภูมิเวกเตอร์ (Vector space) ของ m-tuple บน $GF(q)$ กำหนดเป็น V_m ให้ค่าที่เป็นศูนย์ทั้งหมดของ m-tuple (0, 0, ..., 0) เป็นค่าเริ่มต้นของเรขาคณิต โดยจุดทั้งหมด n หาได้สมการที่ (2.1)

$$n = q^m \tag{2.1}$$

เส้นใน $EG(m,q)$ เป็นทั้งปริภูมิเวกเตอร์หรือโคเซท (Coset) ของปริภูมิย่อย (Subspace) หนึ่งมิติของปริภูมิเวกเตอร์ V_m ของ m-tuple บน $GF(q)$ โดยเส้นทั้งหมดใน $EG(m,q)$ คำนวณได้จากสมการที่ (2.2)

$$J_{EG}(m,1) = q^{m-1}(q^m - 1)/(q-1) \tag{2.2}$$

เส้นทั้งหมดใน $EG(m,q)$ โดยไม่รวมจุดกำเนิด (จุดที่มีค่าเป็น 0) คำนวณหาค่าได้จากสมการที่ (2.3) ดังนี้

$$J_{0,EG}(m,1) = (q^{m-1} - 1)(q^m - 1)/(q-1) \tag{2.3}$$

ให้ $GF(q^m)$ เป็นฟิลด์ขยายของ $GF(q)$ และมีอิลิเมนต์เป็น $\alpha^{-\infty} = 0, \alpha^0 = 1, ..., \alpha^{q^m-2}$ ใน $GF(q^m)$ สำหรับ $EG(m,q)$ ซึ่งมีจุดทั้งหมด $n = q^m$ จุด ให้อิลิเมนต์ 0 เป็นจุดกำเนิดและ α^{j_1} เป็นจุดที่ไม่ใช่จุดกำเนิด เซทของจุด q หาได้ดังนี้

$$\{\beta\alpha^{j_1} : \beta \in GF(q)\} \tag{2.4}$$

ในการหาเส้นของ $EG(m,q)$ ให้ $\beta = 0, 0 \cdot \alpha^{j_1} = 0$ เป็นจุดกำเนิด และให้ α^{j_0} และ α^{j_1} เป็นจุดอิสระจากกัน เส้นหาได้ดังสมการที่ (2.5)

$$\{\alpha^{j_0} + \beta\alpha^{j_1}\} \tag{2.5}$$

<u>ตัวอย่างที่ 2.1</u> พิจารณา $EG(2,2^2)$ บน $GF(2^2)$ คำนวณหาจุดทั้งหมด n จากสมการที่ (2.1) จะได้ $n = q^m = (2^2)^2 = 16$ จุด และจากสมการที่ (2.2) ได้เส้นทั้งหมด 20 เส้น แต่ละเส้นประกอบด้วยจุด

4 จุด เมื่อพิจารณา $GF(2^4)$ มีพหุนามตั้งต้นมีค่าเป็น $1+X+X^4$ บน $GF(2)$ กำหนดให้ α เป็นอิลิเมนต์ตั้งต้น (Primitive element) ของ $GF(2^4)$ และกำหนดให้ $\beta=\alpha^5$

$$GF(2^2)=\{0,\beta^0=1,\beta=\alpha^5,\beta^2=\alpha^{10}\}$$

จากฟิลด์ย่อย (Subfield) $GF(2^2)$ ของ $GF(2^4)$ ทุกอิลิเมนต์ของ α^i ใน $GF(2^4)$ สามารถแสดงในรูปพหุนามได้ดังนี้

$$\alpha^i=\beta_0\alpha^0+\beta_1\alpha,$$

เมื่อ $\beta_0,\beta_1\in GF(2^2)$ ในรูปแบบของเวกเตอร์ α^i แทนใน 2-Tuble (β_0,β_1) บน $GF(2^2)$ ให้ $GF(2^4)$ เป็นฟิลด์ขยาย (Extension field) ของ $GF(2^2)$ ดังตารางที่ 2.4 พิจารณาเรขาคณิตยูคลิดสองมิติ $EG(2,2^2)$ บน $GF(2^2)$ จากสมการที่ (2.4) จะได้

$$L_0=\{\beta_1\alpha\}=\{0,\alpha,\alpha^6,\alpha^{11}\}$$

เมื่อ $\beta_1\in GF(2^2)$ จากสมการที่ (2.5) จะได้

$$L_1=\{1+\beta_1\alpha\}=\{1,\alpha^4,\alpha^{12},\alpha^{13}\}$$
$$L_2=\{\alpha^5+\beta_1\alpha\}=\{\alpha^2,\alpha^3,\alpha^5,\alpha^9\}$$
$$L_3=\{\alpha^{10}+\beta_1\alpha\}=\{\alpha^8,\alpha^7,\alpha^{10},\alpha^{14}\}$$

โดย $L_0,L_1,L_2,$ และ L_3 เป็น Parallel bundle ของเส้นใน $EG(2,2^2)$ และสำหรับทุกจุดใน $EG(2,2^2)$ คำนวณหาเส้นตัดที่จุดเท่ากับ α ได้ดังนี้

$$L'_0=\{\alpha+\beta_1\alpha^2\}=\{\alpha,\alpha^5,\alpha^{13},\alpha^{14}\},$$
$$L'_1=\{\alpha+\beta_1\alpha^3\}=\{\alpha,\alpha^9,\alpha^{10},\alpha^{12}\},$$
$$L'_2=\{\alpha+\beta_1\alpha^4\}=\{1,\alpha,\alpha^3,\alpha^7\},$$
$$L'_3=\{\alpha+\beta_1\alpha^5\}=\{\alpha,\alpha^2,\alpha^4,\alpha^8\},$$
$$L'_4=\{\alpha+\beta_1\alpha^6\}=\{0,\alpha,\alpha^{11},\alpha^6\},$$

เมื่อคำนวณหาจุดตัดของจุดทุกๆค่าทั้งหมดแล้ว ท้ายที่สุดจะได้เส้นทั้ง 20 เส้นตามสมการที่ (2.2) และหากไม่คิดรวมจุดกำเนิด (จุดที่มีค่าเป็น 0) จะได้เส้นทั้งหมด 15 เส้นตามสมการที่ (2.3)

ตารางที่ 2.3 ค่าต่าง ๆ ของ $GF(2^4)$ โดยใช้พหุนามตั้งต้น $1+X+X^4$

i	α^i	พหุนาม	เวกเตอร์
$-\infty$	0	0	0 0 0 0
0	1	1	1 0 0 0
1	α	α	0 1 0 0
2	α^2	α^2	0 0 1 0
3	α^3	α^3	0 0 0 1
4	α^4	$1+\alpha$	1 1 0 0
5	α^5	$\alpha+\alpha^2$	0 1 1 0
6	α^6	$\alpha^2+\alpha^3$	0 0 1 1
7	α^7	$1+\alpha+\alpha^3$	1 1 0 1
8	α^8	$1+\alpha^2$	1 0 1 0
9	α^9	$\alpha+\alpha^3$	0 1 0 1
10	α^{10}	$1+\alpha+\alpha^2$	1 1 1 0
11	α^{11}	$\alpha+\alpha^2+\alpha^3$	0 1 1 1
12	α^{12}	$1+\alpha+\alpha^2+\alpha^3$	1 1 1 1
13	α^{13}	$1+\alpha^2+\alpha^3$	1 0 1 1
14	α^{14}	$1+\alpha^3$	1 0 0 1

ตารางที่ 2.4 ค่าต่าง ๆ ของ $GF(2^4)$ ในฟิลด์ขยาย $GF(2^2)=\{0,1,\beta,\beta^2\}$ เมื่อ $\beta=\alpha^5$

i	α^i	พหุนาม	เวกเตอร์
$-\infty$	0	0	$(0,0)$
0	1	1	$(1,0)$
1	α	α	$(0,1)$
2	α^2	$\beta+\alpha$	$(\beta,1)$
3	α^3	$\beta+\beta^2\alpha$	(β,β^2)
4	α^4	$1+\alpha$	$(1,1)$
5	α^5	β	$(\beta,0)$
6	α^6	$\beta\alpha$	$(0,\beta)$
7	α^7	$\beta^2+\beta\alpha$	(β^2,β)

8	α^8	$\beta^2+\alpha$	$(\beta^2,1)$
9	α^9	$\beta+\beta\alpha$	(β,β)
10	α^{10}	β^2	$(\beta^2,0)$
11	α^{11}	$\beta^2\alpha$	$(0,\beta^2)$
12	α^{12}	$1+\beta^2\alpha$	$(1,\beta^2)$
13	α^{13}	$1+\beta\alpha$	$(1,\beta)$
14	α^{14}	$\beta^2+\beta^2\alpha$	(β^2,β^2)

2.6.2 เรขาคณิตเชิงฉายภาพ

เรขาคณิตเชิงฉายภาพ (Projective Geomety) มีลักษณะที่คล้ายกับเรขาคณิตยูคลิด คือ สร้างจากอิลิเมนต์ของกาลัวส์ฟิลด์ แต่จะหาได้จากการกำหนดจุดขึ้นมา 2 จุด และหาจุดเชื่อมต่ออื่นๆระหว่างจุด 2 จุดนั้น โดยเรขาคณิตเชิงฉายภาพ $PG(m,q)$ กระทำบนกาลัวส์ฟิลด์ $GF(q^{m+1})$ และจำนวนจุดทั้งหมดของเรขาคณิตเชิงฉายภาพหาได้ดังนี้

$$n=\frac{q^{m+1}-1}{q-1} \tag{2.6}$$

จำนวนเส้นทั้งหมด ดังสมการที่ (2.7)

$$(\alpha^i)=\{\alpha^i,\beta\alpha^i,...,\beta^{q-2}\alpha^i\} \tag{2.7}$$

โดย $0\le i<n$ และการคำนวณหาจุดทั้งหมดในเส้นจากส่วนขยายกาลัวส์ หาได้จากสมการที่ (2.8)

$$\eta_1\alpha^i+\eta_2\alpha^j \tag{2.8}$$

โดย $\eta_1,\eta_2\in\{0,1,\beta,...,\beta^{q-2}\}$ และ $i\neq j$

<u>ตัวอย่างที่ 2.2</u> พิจารณา $PG(2,2^2)$ บน $GF(64)$ คำนวณหาจุดทั้งหมด n จากสมการที่ (2.6) จะได้ $n=\frac{(2^2)^{2+1}-1}{(2^2)-1}=21$ จุด โดย α เป็นพหุนามของ $GF(64)$ ให้ $\beta=\alpha^{21}$ และจากฟิลด์ย่อย $GF(2^2)=\{0,1,\beta,\beta^2\}$ จากนั้นคำนวณหาจุดทั้งหมดจากสมการที่ (2.7) จะประกอบด้วยจุดดังต่อไปนี้คือ $\alpha^0,\alpha^1,\alpha^2,...,\alpha^{20}$ ต่อไปให้คำนวณหาเส้นที่ผ่านจุด 2 จุด ในที่นี้ยกตัวอย่างหาจุดจาก (α) และ (α^{20}) ในการคำนวณให้คำนวณตามสมการที่ (2.8) พิจารณาจากตารางพหุนามของ

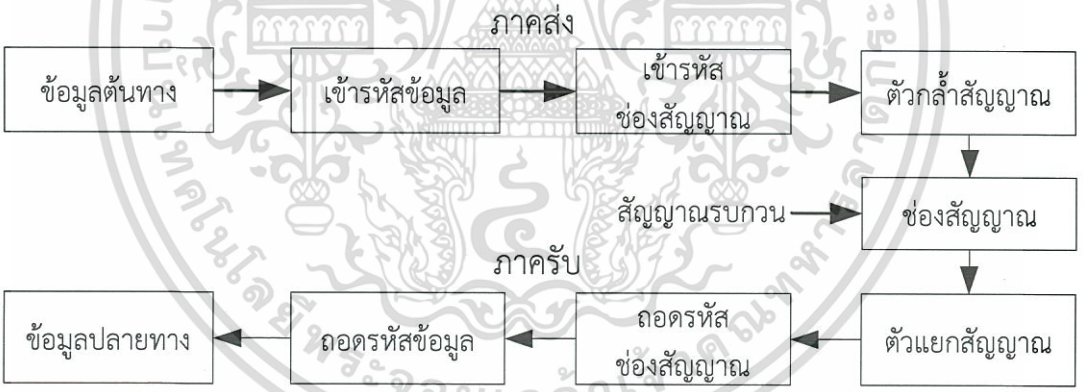
$GF(64)$ และเมื่อได้คำตอบแล้วให้หากค่า α มีค่ายกกำลังมากกว่า $\beta = \alpha^{21}$ ให้ทำการมอดูโลค่าที่ได้ด้วย 21 เนื่องจากจุดทั้งหมดมี 21 จุด ดังเช่นตัวอย่างต่อไปนี้

$$
\begin{aligned}
&(\alpha),\\
&(\alpha^{20}),\\
&(\alpha+\alpha^{20}) = (\alpha^{57}) = (\alpha^{15}),\\
&(\alpha+\beta\alpha^{20}) = (\alpha+\alpha^{41}) = (\alpha^{56}) = (\alpha^{14}),\\
&(\alpha+\beta^2\alpha^{20}) = (\alpha+\alpha^{62}) = (\alpha^{11})
\end{aligned}
$$

เมื่อ $\{(\alpha),(\alpha^{11}),(\alpha^{14}),(\alpha^{15}),(\alpha^{20})\}$ เป็นจุดทั้งหมดของเส้น $PG(2,2^2)$ ที่ผ่านจุด (α) และ (α^{20}) หลังจากนั้นให้ทำการหาเส้นที่ผ่านจุดทั้งหมดจบครบจากเส้นทั้งหมด n เส้น

2.7 พื้นฐานระบบสื่อสารดิจิทัล

พื้นฐานระบบสื่อสารดิจิทัลหรือระบบจัดเก็บข้อมูลดิจิทัลโดยทั่วไปจะประกอบด้วย ภาคส่ง และภาครับ โดยสามารถจำลองเป็นแผนภาพทั่วไปได้ดังรูปที่ 2.1



รูปที่ 2.1 แผนภาพพื้นฐานระบบสื่อสารดิจิทัลหรือระบบจัดเก็บข้อมูลดิจิทัล

จากรูปที่ 2.1 ข้อมูลต้นทาง (Source) และข้อมูลปลายทาง (Sink) คือบิตข้อมูลที่ต้องการส่งและข้อมูลที่ได้รับปลายทาง โดยข้อมูลในระบบสื่อสารหรือข้อมูลที่ต้องการจัดเก็บในระบบจัดเก็บข้อมูลจะอยู่ในรูปสัญญาณแอนะล็อก (Analog signal) เช่น ข้อมูลเสียง และแปลงเป็นสัญญาณดิจิทัล (Digital signal) หรืออยู่ในรูปแบบสัญญาณดิจิทัลโดยตรง เช่น ข้อมูลจากไฟล์คอมพิวเตอร์

การเข้ารหัสข้อมูลต้นทาง (Source encoder) เป็นการเข้ารหัสโดยกระบวนการเปลี่ยนแปลงบิตข้อมูลต้นทางให้อยู่ในลำดับบิต (Bit sequence) ในรูปแบบอื่นเพื่อลดความซ้ำซ้อนของข้อมูลต้นทางโดยวิธีการบีบอัด (Compression) ซึ่งมี 2 ประเภท คือ การบีบอัดโดยปราศจากการสูญเสีย (Lossless) เช่น ข้อมูลจากไฟล์คอมพิวเตอร์ และการบีบอัดแบบมีการสูญเสีย (Lossy) เช่น

ข้อมูลภาพหรือเสียงที่ยินยอมให้มีการสูญเสียข้อมูลบางส่วนได้ เป็นต้น การเข้ารหัสด้วยวิธีนี้ทำให้ได้ข้อมูลเอาท์พุตที่มีจำนวนบิตน้อยกว่าข้อมูลต้นทาง ซึ่งทำให้อัตราข้อมูล (data rate) และแบนด์วิดท์ (bandwidth) ที่ต้องการใช้งานลดลง สำหรับการถอดรหัสข้อมูลต้นทาง (Source decoder) เป็นกระบวนการถอดรหัสเพื่อให้ได้ข้อมูลเดียวกันกับข้อมูลต้นทางในกรณีที่มีการบีบอัดโดยปราศจากการสูญเสีย หรือเป็นการถอดรหัสเพื่อให้ได้ค่าที่ใกล้เคียงกับข้อมูลต้นทางในกรณีที่มีการบีบอัดแบบมีการสูญเสีย

การเข้ารหัสช่องสัญญาณ (Channel encoder) และการถอดรหัสช่องสัญญาณ (Channel decoder) เพื่อลดอัตราข้อผิดพลาดของข้อมูล ในการเข้ารหัสจะใช้ข้อมูลต้นทางที่เข้ารหัสข้อมูลแล้วหรือเรียกอีกอย่างหนึ่งว่าข้อความ (Message) ทำการเข้ารหัสเพื่อสร้างข้อมูลชุดใหม่เรียกว่าคำรหัส (Codeword) ซึ่งประกอบด้วยข้อมูลข้อความและข้อมูลการตรวจสอบด้วยส่วนซ้ำซ้อน (Redundant Check) และอัตราส่วนระหว่างข้อมูลข้อความต่อคำรหัสเรียกว่า อัตรารหัส (Code rate)

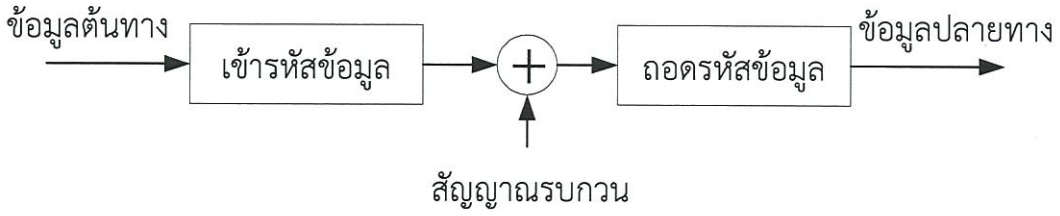
ตัวกล้ำสัญญาณ (Modulator) เป็นการปรับรูปสัญญาณให้เกิดความเหมาะสมในการส่งสัญญาณผ่านช่องสัญญาณ และตัวแยกสัญญาณ (Demodulator) เป็นการแยกสัญญาณข้อมูลออกจากสัญญาณที่ได้รับมาจากช่องสัญญาณก่อนเข้ากระบวนการถอดรหัสเพื่อลดอัตราการผิดพลาดของข้อมูล

ช่องสัญญาณ (Channel) คือตัวกลางทางกายภาพ เช่น สายนำสัญญาณ อากาศ หรือแผ่นมีเดีย (Media) ในฮาร์ดดิสก์ไดรฟ์ ช่องสัญญาณทำหน้าที่เป็นตัวกลางในการส่งผ่านข้อมูลจากต้นทางไปยังปลายทาง โดยข้อมูลที่ผ่านช่องสัญญาณจะได้รับผลกระทบต่าง ๆ จากสัญญาณรบกวนทำให้สัญญาณที่ส่งมีความผิดเพี้ยน

สัญญาณรบกวน (Noise) เป็นสัญญาณที่ระบบไม่ต้องการ หากสัญญาณรบกวนมากจะทำให้เกิดข้อผิดพลาดของข้อมูลมากก่อนเข้าภาครับ ซึ่งอาจส่งผลให้การแก้ไขข้อมูลผิดพลาดไม่สามารถจะแก้ไขข้อมูลให้ถูกต้องได้ โดยทั่วไปสัญญาณรบกวนมีหลายประเภท เช่น สัญญาณรบกวนเกาส์เซียน (Gaussian noise), สัญญาณรบกวนเชิงความร้อน (Thermal noise) และ สัญญาณรบกวนอิเลคทรอนิกส์ (Electronics noise) เป็นต้น

2.8 ช่องสัญญาณเกาส์เซียน

สัญญาณเกาส์เซียนหรือสัญญาณรบกวนแบบสีขาว (AWGN Channel) พบมากในระบบการประมวลผลสัญญาณของระบบบันทึกข้อมูล และการสื่อสารข้อมูล ตัวอย่างเช่น สัญญาณรบกวนจากความร้อน ส่งผลให้การทำงานของวงจรภาครับเกิดความผิดพลาดขึ้นดังนั้นในการทดสอบสมรรถนะของรหัสแอลดีพีซี จึงได้ทำการทดสอบภายใต้ระบบที่มีสัญญาณรบกวนแบบสีขาว ตัวแปรสุ่มแบบเกาส์เซียน (Gaussian random variable) เป็นที่นิยมใช้งานในการวิเคราะห์ระบบสื่อสาร ทั้งนี้เนื่องจากพฤติกรรมของตัวแปรสุ่มแบบเกาส์เซียนมีลักษณะคล้ายกับข้อมูลที่รับส่งภายในระบบสื่อสาร เช่น สัญญาณรบกวนและข้อมูลข่าวสาร เป็นต้น



รูปที่ 2.2 แผนภาพจำลองช่องสัญญาณเกาส์เซียน

ในการทดสอบการกล้ำสัญญาณ Binary phase-shift keying หรือ BPSK กำหนดได้ดังนี้

$$y = ax + n \tag{2.9}$$

เมื่อ a คือ แอมพลิจูด (สำหรับช่องสัญญาณเกาส์เซียนจะกำหนดให้แอมพลิจูดมีค่าเท่ากับ 1),

x คือ สัญญาณที่ผ่านการกล้ำสัญลักษณ์ (Modulation Symbol) มีค่าเป็น $+1$ หรือ -1 ,

n คือ สัญญาณรบกวนในช่องสัญญาณเกาส์เซียนโดยที่มีค่าการแจกแจง Pdf ดังสมการที่ (2.10)

$$n \sim N(0, \sigma^2) \tag{2.10}$$

ค่าความแปรปรวน (Variance) หาได้ดังสมการที่ (2.11)

$$\sigma^2 = \frac{N_0}{2} \tag{2.11}$$

โดยที่ N_0 คือ ความหนาแน่นสเปกตรัมกำลังของสัญญาณรบกวน (Noise power spectrum density)

$$\sigma^2 = \frac{N_0}{2} \tag{2.12}$$

โดยที่

$$\frac{E_b}{N_0} = \frac{E_s}{R_m R_c N_0} = \frac{E_s}{R_m R_c 2\sigma^2} = \frac{1}{R_m R_c N_0} \tag{2.13}$$

เมื่อ E_b คือ คือพลังงานต่อบิต (Bit Energy),

E_s คือ พลังงานต่อสัญลักษณ์ (Symbol Energy) หากส่งครั้งละ 1 บิตแล้ว $E_b = E_s$,

$R_m = \log_2(M)$ เมื่อกล้ำสัญญาณสัญลักษณ์แบบ BPSK ได้ $M = 2$, QPSK ได้ $M = 4$ และ 16 QAM ได้ $M = 16$ โดย R_m คือขนาดของบิตต่อสัญลักษณ์

R_c คือ อัตรารหัส

ดังนั้นค่าความแปรปรวนของสัญญาณรบกวนจะได้เป็น

$$\sigma^2 = \left(2R_m R_c \frac{E_b}{N_0} \right)^{-1} \tag{2.14}$$

ในกรณีกล้ำสัญญาณสัญลักษณ์แบบ BPSK ค่าความแปรปรวนของสัญญาณรบกวนมีค่าเป็น

$$\sigma^2 = \left(2R_c \frac{E_b}{N_0} \right)^{-1} \tag{2.15}$$

จากรูปที่ 2.2 การคำนวณหาค่าอัตราบิตผิดพลาด (Bit Error Rate หรือ BER) หาได้จากจำนวนบิตผิดพลาดจากฝั่งรับต่อสัญญาณบิตทั้งหมดที่ส่งออกไป ดังสมการที่ (2.16)

$$\text{BER} = \frac{\text{บิตผิดพลาดสะสมที่รหัสแอลดีพีซีแก้ไขไม่ได้}}{\text{บิตที่ทำการส่งเพื่อทดสอบรหัสแอลดีพีซีทั้งหมด}} \tag{2.16}$$

ส่วนการคำนวณหาค่าอัตราเฟรมผิดพลาด (Frame Error Rate หรือ FER) หาได้ดังสมการที่ (2.17)

$$\text{FER} = \frac{\text{ข้อมูลเฟรมผิดพลาด สะสมที่รหัสแอลดีพีซีแก้ไขไม่ได้}}{\text{ข้อมูลเฟรมผิดพลาดที่ทำการส่งเพื่อทดสอบรหัสแอลดีพีซีทั้งหมด}} \tag{2.17}$$

2.9 รหัสบล็อก

รหัสบล็อก (Block Codes) คือ รหัสแก้ไขข้อมูลผิดพลาด โดยข้อมูลข่าวสารที่มีขนาดข้อมูล k บิต จะถูกเข้ารหัส (Encode) ทำให้เกิดบิตข้อมูลตรวจสอบ (Parity bits) จำนวน $n-k$ บิต โดยรหัสบล็อกสามารถแบ่งออกได้เป็น 2 ประเภท คือ รหัสบล็อกเชิงเส้น (Linear block codes) และรหัสบล็อกไม่เชิงเส้น (Nonlinear block codes) แต่โดยทั่วไปนิยมใช้รหัสบล็อกเชิงเส้นและในวิทยานิพนธ์นี้จะกล่าวถึงเฉพาะรหัสบล็อกเชิงเส้นเท่านั้น คุณสมบัติที่สำคัญของรหัสบล็อกมีดังนี้

- อัตรารหัส (Code rate) คือ อัตราส่วนระหว่างขนาดข้อมูลที่ต้องการส่ง (message) k ต่อขนาดของคำรหัส (Codeword) n โดยอัตรารหัส R มีค่าเป็น

$$R = k/n \tag{2.18}$$

- น้ำหนักคำรหัส (Code Word Weight) คือ จำนวนที่มีค่าไม่เท่ากับศูนย์ของคำรหัส เช่น คำรหัสมีค่าเป็น (1011001) ดังนั้นน้ำหนักคำรหัสนี้มีค่าเท่ากับ 4 (มี "1" อยู่ 4 ตัวอยู่ในคำรหัส)

- ระยะห่างแฮมมิง (Hamming distance) คือ การเปรียบเทียบค่าจำนวนที่ไม่ใช่ศูนย์ของคำรหัส 2 ชุดว่ามีความแตกต่างกันเท่าใด ซึ่งสามารถหาได้จากสมการดังนี้

$$d_{\text{Hamming}}(v,w) = d(v,w) = |\{i \mid v_i \neq w_i,\ \ i = 0,1,...,n-1\}| \tag{2.19}$$

ตัวอย่างที่ 2.3 รหัสบล็อกมีคำรหัสทั้งหมด 2 ชุด คือ $v = (00100)$ และ $w = (10010)$ ดังนั้นแล้ว $v \oplus w = (10110)$ ดังนั้นระยะห่างแฮมมิง $d_{\text{Hamming}}(v,w) = 3$

- ระยะห่างต่ำสุด (Minimum distance) ของรหัสบล็อก คือ การเปรียบเทียบค่าจำนวนที่ไม่ใช่ศูนย์ของคำรหัสของคำรหัสหลายชุด และคำนวณเช่นเดียวกับระยะห่างแฮมมิง เพียงแต่จะเลือกค่าต่ำสุดที่ได้เป็นคำตอบ โดยระยะห่างต่ำสุดของรหัสสามารถที่จะตรวจจับบิตผิดพลาดของข้อมูลได้น้อยกว่าหรือเท่ากับ $d_{\min} - 1$ นอกจากนั้นระยะห่างต่ำสุดสามารถที่จะบอกได้ถึงบิตที่สามารถแก้ไขได้สูงสุดเท่ากับ $(d_{\min} - 1)/2$

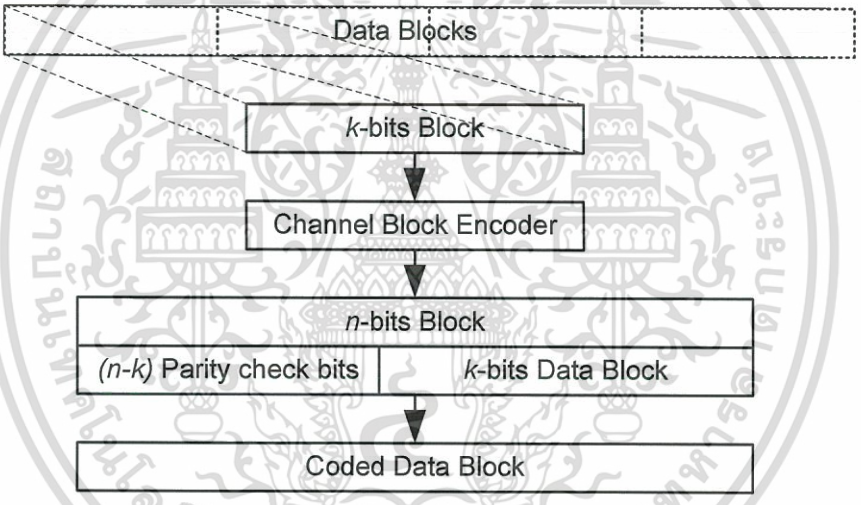
ตัวอย่างที่ 2.4 รหัสบล็อกมีคำรหัสทั้งหมด 4 ชุด มีค่าดังนี้
$c = \{(01100), (10001), (00010), (11111)\}$ ให้ทำการเปรียบเทียบผลต่างของคำรหัสแต่ละชุดดังนี้

ระยะห่างแฮมมิงระหว่าง (01100) และ (10001) ได้ $d_{\text{Hamming}} = 4$
ระยะห่างแฮมมิงระหว่าง (01100) และ (00010) ได้ $d_{\text{Hamming}} = 3$
ระยะห่างแฮมมิงระหว่าง (01100) และ (11111) ได้ $d_{\text{Hamming}} = 3$
ระยะห่างแฮมมิงระหว่าง (10001) และ (00010) ได้ $d_{\text{Hamming}} = 3$
ระยะห่างแฮมมิงระหว่าง (10001) และ (11111) ได้ $d_{\text{Hamming}} = 3$
ระยะห่างแฮมมิงระหว่าง (00010) และ (11111) ได้ $d_{\text{Hamming}} = 3$

ระยะห่างต่ำสุดคือค่าระยะห่างแฮมมิงที่ต่ำสุด ดังนั้นระยะห่างต่ำสุด $d_{\min} = 3$ และความสามารถในการแก้ไขข้อมูลผิดพลาดสูงสุดเท่ากับ $(3-1)/2 = 1$ บิต

2.10 รหัสบล็อกเชิงเส้น

รหัสบล็อกเชิงเส้นจะทำการแบ่งบิตข้อมูล (information bits) ออกเป็นบล็อกที่มีขนาดเท่ากัน โดยในแต่ละบล็อกข้อมูลจะมีบิตข้อมูลเป็นจำนวน k บิต ทำให้ข้อมูลที่จะถูกนำไปเข้าวงจรเข้ารหัส (Encoder) และในภายหลังการเข้ารหัสจะได้ข้อมูลชุดใหม่ซึ่งจะเรียกว่าคำรหัส (Codeword) ขนาด n บิต โดยบิตจำนวน $n-k$ บิต หรือบิตพาริตี้ (Parity bits) ที่ถูกเพิ่มเข้าไปนี้จะทำหน้าที่ในการตรวจจับ และแก้ไขความผิดพลาดจากสัญญาณรบกวนที่มีอยู่ในช่องสัญญาณ ทั้งนี้นิยมเขียนอธิบายคุณลักษณะของรหัสบล็อกในรูปของ (n,k) กระบวนการเข้ารหัสของรหัสบล็อกเชิงเส้นมีรูปแบบดังรูปที่ 2.3



รูปที่ 2.3 กระบวนการเข้ารหัสของรหัสบล็อกเชิงเส้น

รหัสบล็อกเชิงเส้นมีคุณสมบัติที่สำคัญมี 2 อย่างคือ

1. ผลบวกของคำรหัสใดๆ 2 ชุด จะได้ผลลัพธ์ที่เป็นคำรหัสด้วย
2. ระยะห่างต่ำสุด (Minimum distance) มีค่าเท่ากับน้ำหนักต่ำสุด (Minimum weigh) ของคำรหัสที่มีจำนวนค่าที่ไม่ใช่ศูนย์ โดยแบ่งได้เป็น

- ขอบเขตซิงเกิลตัน (Singleton Bound) : รหัสบล็อกเชิงเส้น (n,k) มีระยะห่างต่ำสุด (Minimum distance) ของรหัสบล็อก คือ

$$d_{\min} = n - k + 1 \tag{2.20}$$

- ขอบเขตแฮมมิง (Hamming Bound) : รหัสบล็อกเชิงเส้น (n,k) สามารถแก้ไขข้อมูลผิดพลาดได้ t บิต โดยมีเงื่อนไขดังสมการต่อไปนี้

$$2^{n-k} \geq \sum_{i=0}^{t} \binom{n}{i} \tag{2.21}$$

โดยความสัมพันธ์ระหว่าง Upper bound ของระยะห่างต่ำสุดและ Hamming Bound ดังสมการ

$$\binom{n}{i} = \frac{n!}{(n-i)!i!},\ t = (d_{\min} - 1)/2 \tag{2.22}$$

2.11 เมทริกซ์กำเนิดและเมทริกซ์ตรวจสอบพาริตี้

เมทริกซ์กำเนิด (Generator Matrices) คือเมทริกซ์ที่ใช้สำหรับสร้างคำรหัสจากข้อมูลอินพุท ให้ $\{g_0, g_1, ..., g_{k-1}\}$ สำหรับรหัสบล็อก (n,k) และให้ข้อมูลอินพุท $\mathbf{m} = \{m_0, m_1, ..., m_{k-1}\}$ เป็นข้อมูลที่ใช้ในการเข้ารหัส เมื่อเข้ารหัสจะได้คำรหัส $c = \{c_0, c_1, ..., c_{k-1}\}$

$$\mathbf{c} = m_0 g_0 + \cdots + m_{k-1} g_{k-1} \tag{2.23}$$

เมทริกซ์กำเนิดแบบเชิงระบบ (Systematic) จะอยู่ในรูปสมการที่ (2.24)

$$\mathbf{G} = [\mathbf{P} \vdots \mathbf{I}_k]_{k \times n} \tag{2.24}$$

โดย $\mathbf{I}_k$ คือเมทริกซ์เอกลักษณ์ จากสมการที่ (2.24) สามารถเขียนสมการใหม่ได้เป็น

$$\mathbf{G} = \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0,0} & g_{0,1} & \cdots & g_{0,n-1} \\ g_{1,0} & g_{1,1} & \cdots & g_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & \cdots & g_{k-1,n-1} \end{bmatrix} \tag{2.25}$$

โดย $g_i, 0 \leq i \leq k-1$ เป็นเวกเตอร์ในแต่ละแถวของเมทริกซ์กำเนิด $\mathbf{G}$ และเมทริกซ์กำเนิดสำหรับสร้างคำรหัสสามารถทำการเข้ารหัสได้โดยตรงดังนี้

$$\mathbf{mG} = (m_0, m_1, ..., m_{k-1}) \begin{bmatrix} g_0 \\ g_1 \\ \vdots \\ g_{k-1} \end{bmatrix} = m_0 g_0 + m_1 g_1 + ... + m_{k-1} g_{k-1} = \mathbf{c} \tag{2.26}$$

ให้เมทริกซ์ตรวจสอบพาริตี้มีโครงสร้างเป็น

$$\mathbf{H} = \begin{bmatrix} h_0 \\ h_1 \\ \vdots \\ h_{n-k-1} \end{bmatrix} = \begin{bmatrix} h_{0,0} & h_{0,1} & \cdots & h_{0,n-1} \\ h_{1,0} & h_{1,1} & \cdots & h_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ h_{n-k-1,0} & h_{n-k-1,1} & \cdots & h_{n-k-1,n-1} \end{bmatrix} \tag{2.27}$$

ในรหัสบล็อกเชิงเส้นที่มีการเข้ารหัสเชิงระบบ คำรหัสจากตำแหน่ง $n-k$ จนถึงตำแหน่ง n มีค่าดังสมการ (2.28) หรือก็คือคำรหัสในช่วงตำแหน่งดังกล่าวก็คือข้อมูลข้อมูลอินพุท m

$$c_i = m_{i-(n-k)}, \; i = n-k, ..., n \tag{2.28}$$

ส่วนข้อมูลของคำรหัสจากตำแหน่งที่ 0 จนถึงตำแหน่ง $n-k-1$ เป็นข้อมูลในส่วนของบิตพาริตี้ ซึ่งมีสมการดังนี้

$$\begin{aligned} c_0 &= p_{0,0} m_0 + p_{1,0} m_1 + \cdots + p_{k-1,0}, m_{k-1} \\ c_1 &= p_{0,1} m_0 + p_{1,1} m_1 + \cdots + p_{k-1,1}, m_{k-1} \\ &\vdots \\ c_{n-k-1} &= p_{0,n-k-1} m_0 + p_{1,n-k-1} m_1 + \cdots + p_{k-1,n-k-1}, m_{k-1} \end{aligned} \tag{2.29}$$

จากสมการที่ (2.28) และ (2.29) สามารถเขียนให้อยู่ในรูปของเมทริกซ์ ดังนี้

$$[c_0, c_1, ..., c_n] = [m_0, m_1, ..., m_{k-1}] \begin{bmatrix} p_{0,0} & p_{0,1} & \cdots & p_{0,n-k-1} & 1000 & \cdots & 0 \\ p_{1,0} & p_{1,1} & \cdots & p_{1,n-k-1} & 0100 & \cdots & 0 \\ \vdots & \vdots & & & \vdots & \vdots & \vdots \\ p_{k-1,0} & p_{k-1,1} & \cdots & p_{k-1,n-k-1} & 0000 & & 1 \end{bmatrix} \tag{2.30}$$

หรือ คำรหัสได้จาก

$$\mathbf{c} = \mathbf{m} \times \mathbf{G} \tag{2.31}$$

จากสมการที่ (2.30) หากพิจารณาเมทริกซ์กำเนิดทางด้านขวา ซึ่งเป็นรูปแบบของเมทริกซ์เอกลักษณ์ เมทริกซ์กำเนิดจะมีรูปแบบดังสมการที่ (2.32)

$$\mathbf{G} = [\mathbf{P} \vdots \mathbf{I}_k]_{k \times n} \tag{2.32}$$

ดังนั้นเมทริกซ์ตรวจสอบพาริตี้สำหรับการถอดรหัสเชิงระบบได้ดังสมการที่ (2.33)

$$\mathbf{H} = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & p_{0,0} & p_{1,0} & \cdots & p_{k-1,0} \\ 0 & 1 & 0 & 0 & 0 & p_{0,1} & p_{1,1} & \cdots & p_{k-1,1} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 1 & p_{0,n-1} & p_{1,n-1} & \cdots & p_{k-1,n-1} \end{bmatrix} \tag{2.33}$$

โดยเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ แบบสมมาตรสามารถแยกออกเป็นเมทริกซ์เอกลักษณ์ที่มีขนาด $(n-k)\times(n-k)$ $\mathbf{I}_{n-k}$ และทรานโพสเมทริกซ์สำหรับค่าบิตตรวจสอบ $\mathbf{P}^T$ ดังสมการที่ (2.34)

$$\mathbf{H} = [\mathbf{I}_{n-k} \vdots \mathbf{P}^T] \tag{2.34}$$

เมื่อนำเมทริกซ์กำเนิดมาทำการคูณกับเมทริกซ์ตรวจสอบพาริตี้จะได้ค่าเป็นเมทริกซ์ศูนย์ ดังสมการที่ (2.35)

$$\mathbf{G} \times \mathbf{H}^T = 0 \tag{2.35}$$

หากคำรหัสที่ผ่านวงจรถอดรหัสแล้วทำการการคูณด้วยทรานโพสเมทริกซ์ตรวจสอบพาริตี้และได้ค่าเป็นเวกเตอร์ศูนย์ แสดงว่าการถอดรหัสสามารถถอดรหัสได้อย่างถูกต้อง ดังสมการที่ (2.27)

$$\mathbf{c}\mathbf{H}^T = 0 \tag{2.36}$$

2.12 การตรวจจับข้อผิดพลาดและการถอดรหัสซินโดรมของรหัสบล็อกเชิงเส้น

การตรวจจับข้อผิดพลาดของรหัสบล็อกเชิงเส้น (n,k) จากเมทริกซ์กำเนิดและเมทริกซ์ตรวจสอบพาริตี้ ให้ $\mathbf{c} = \{c_0, c_1, ..., c_{k-1}\}$ เป็นคำรหัสที่ได้จากการเข้ารหัสก่อนส่งผ่านช่องสัญญาณรบกวน และให้ $\mathbf{r} = (r_0, r_1, ...r_{k-1})$ เป็นข้อมูลฝั่งรับที่ผ่านช่องสัญญาณรบกวนและพิจารณาถอดรหัสแบบหยาบ (Hard decision) ให้อยู่ในรูปแบบข้อมูลแบบไบนารี และในการหาตำแหน่งข้อมูลผิดพลาดสามารถหาได้จากสมการที่ (2.37)

$$\mathbf{r} = \mathbf{c} + \mathbf{e} \tag{2.37}$$

และการคำนวณหาค่าซินโดรม $\mathbf{s}$ สามารถหาได้จากสมการที่ (2.38)

$$\begin{aligned} \mathbf{s} &= \mathbf{r} \cdot \mathbf{H}^T \\ &= (\mathbf{c} + \mathbf{e}) \times \mathbf{H}^T \\ &= \mathbf{c} \times \mathbf{H}^T + \mathbf{e} \times \mathbf{H}^T \\ &= \mathbf{0} + \mathbf{e} \times \mathbf{H}^T \\ &= \mathbf{e} \times \mathbf{H}^T \end{aligned} \tag{2.38}$$

จากสมการที่ (2.38) ในกรณีที่ $\mathbf{e}$ ไม่มีข้อมูลผิดพลาดค่าซินโดรมที่ได้จะมีค่าเป็นศูนย์ โดยค่าซินโดรม $\mathbf{s}$ และแพทเทิร์นบิตผิดพลาด $\mathbf{e}$ มีขนาดเป็น

$$\mathbf{s} = s_0, s_1, \ldots, s_{n-1} \tag{2.39}$$

$$\mathbf{e} = e_0, e_1, \ldots, e_{n-1} \tag{2.40}$$

2.13 รหัสแฮมมิง

รหัสแฮมมิง (Hamming codes) เป็นรหัสบล็อกเชิงเส้นแบบไบนารีที่มีความสามารถในการตรวจจับข้อมูลผิดพลาดและสามารถแก้ไขข้อมูลผิดพลาดได้ 1 บิต และมีระยะห่างต่ำสุด (Minimum distance) $d_{\min} = 3$ โดยคุณสมบัติของรหัสแฮมมิงมีดังนี้

ความยาวรหัส	$n = 2^m - 1$
จำนวนบิตข้อมูล	$k = 2^m - m - 1$
จำนวนเช็คบิต	$m = n - k$
สามารถแก้ไขข้อมูลผิดพลาด	$t = 1$

จากหัวข้อที่ได้กล่าวมาก่อนหน้านี้ในส่วนของการเข้ารหัสและการถอดรหัส การตรวจจับข้อผิดพลาดและการถอดรหัสซินโดรม ในหัวข้อนี้จะแสดงให้เห็นถึงขั้นตอนการถอดรหัสซินโดรมของรหัสแฮมมิง

<u>ตัวอย่างที่ 2.5</u> รหัสแฮมมิง (7, 4) กำหนดให้มีเมทริกซ์กำเนิดและเมทริกซ์ตรวจสอบพาริตี้ ดังนี้

$$\mathbf{G}=\begin{bmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&1&0&0&1&0\\1&0&1&0&0&0&1\end{bmatrix},\ \mathbf{H}=\begin{bmatrix}1&0&0&1&0&1&1\\0&1&0&1&1&1&0\\0&0&1&0&1&1&1\end{bmatrix}$$

ป้อนข้อมูลอินพุทเป็นศูนย์ทั้งหมดจำนวน 4 บิต $\mathbf{m}=[0\ 0\ 0\ 0]$ เมื่อทำการเข้ารหัสด้วยเมทริกซ์กำเนิดจะได้คำรหัสที่มีค่าเป็นศูนย์ทั้งหมด 7 บิต $\mathbf{c}=[0\ 0\ 0\ 0\ 0\ 0\ 0]$ และรหัสแฮมมิงมีความสามารถในการแก้ไขบิตผิดพลาดได้ 1 บิต ดังนั้นการหาจำนวนแพทเทิร์นบิตบิตผิดพลาดจะเท่ากับ $2^{(7-4)}=8$ รูปแบบ จากสมการที่ (2.37) เมื่อ $\mathbf{r}=\mathbf{c}+\mathbf{e}$ ให้นำค่าคำรหัส $\mathbf{c}$ ทำการบวกแบบมอดูโลกับแพทเทิร์นบิตผิดพลาด $\mathbf{e}$ เพื่อหาค่าซินโดรม และจากสมการที่ (2.29) ทำการคำนวณหาค่าซินโดรม ได้ค่าซินโดรมดังตารางที่ 2.5

ดังนั้นการนำรหัสแฮมมิงไปใช้งานจะพิจารณาจากซินโดรม หากค่าซินโดรมที่ได้มีค่าที่ไม่ใช่เวกเตอร์ศูนย์ $\mathbf{s}\neq[0\ 0\ 0]$ แสดงว่าข้อมูลที่ได้รับมีข้อผิดพลาด ให้นำข้อมูลที่ได้รับมาทำการบวกแบบมอดูโลกับแพทเทิร์นบิตผิดพลาดและทำการตรวจสอบค่าซินโดรมอีกครั้ง หากค่าซินโดรมที่ได้ใหม่มีค่าเป็นเวกเตอร์ศูนย์ $\mathbf{s}=[0\ 0\ 0]$ แสดงว่ามีข้อผิดพลาด 1 บิตและตำแหน่งบิตผิดพลาดตรวจสอบได้จากตาราง หากค่าซินโดรมที่ได้ไม่ใช่เวกเตอร์ศูนย์หมายถึงบิตผิดพลาดมากกว่า 1 บิตและรหัสแฮมมิงไม่สามารถที่จะแก้ไขข้อมูลดังกล่าวได้ เนื่องจากเกินขอบเขตความสามารถในการแก้ไขข้อมูลของรหัสแฮมมิง

ตารางที่ 2.5 แพทเทิร์นบิตผิดพลาดและค่าซินโดรมจากตัวอย่าง รหัสแฮมมิง (7,4)

แพทเทิร์นบิตผิดพลาด (e)	ค่าซินโดรม (s)
0 0 0 0 0 0 0	0 0 0
1 0 0 0 0 0 0	1 0 0
0 1 0 0 0 0 0	0 1 0
0 0 1 0 0 0 0	0 0 1
0 0 0 1 0 0 0	1 1 0
0 0 0 0 1 0 0	0 1 1
0 0 0 0 0 1 0	1 1 1
0 0 0 0 0 0 1	1 0 1

2.14 รหัสไซคลิค

รหัสไซคลิก (Cyclic codes) เป็นรหัสบล็อกเชิงเส้นชนิดหนึ่ง เมื่อนำคำรหัสหนึ่งมาเลื่อนบิตแบบวนกลับแล้วจะต้องได้ผลลัพธ์ที่เป็นคำรหัสด้วย ในส่วนของฮาร์ดแวร์โครงสร้างวงจรเข้ารหัสของรหัสไซคลิกเป็นวงจรที่มีลักษณะการเข้ารหัสได้ง่ายโดยที่อาศัยการใช้เรจิสเตอร์แบบเลื่อน (Shift Registers) เชื่อมต่อกันและทำการป้อนกลับ (Feedback) เรียกว่าการเรจิสเตอร์แบบเลื่อนแบบป้อนกลับเชิงเส้น (Linear Feedback Shift Register: LFSR)

ให้คำรหัสเวกเตอร์ $\mathbf{c} = (c_0, c_1, \ldots c_{t-1})$ สามารถเขียนอยู่ในรูปของพหุนามดีกรี $n-1$ ได้พหุนามรหัส (Code Polynomial) ดังสมการที่ (2.41)

$$\mathbf{c}(x) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1} \tag{2.41}$$

ข้อความที่ต้องการส่งหรือเวกเตอร์ $\mathbf{m}$ สามารถเขียนอยู่ในรูปของพหุนามดีกรี $n-1$ ได้พหุนามข้อความ (Massage Polynomial) ดังสมการที่ (2.42)

$$\mathbf{m}(x) = m_0 + m_1 x + \cdots + m_{n-1} x^{n-1} \tag{2.42}$$

และพหุนามกำเนิด (Generator Polynomial) ดังสมการที่ (2.43)

$$\mathbf{g}(x) = 1 + g_1 x + g_2 x^2 + \cdots + g_{n-k-1} x^{n-k-1} + x^{n-k} \tag{2.43}$$

ดังนั้นพหุนามข้อความคูณกับพหุนามกำเนิด จะได้พหุนามรหัส ดังสมการที่ (2.44)

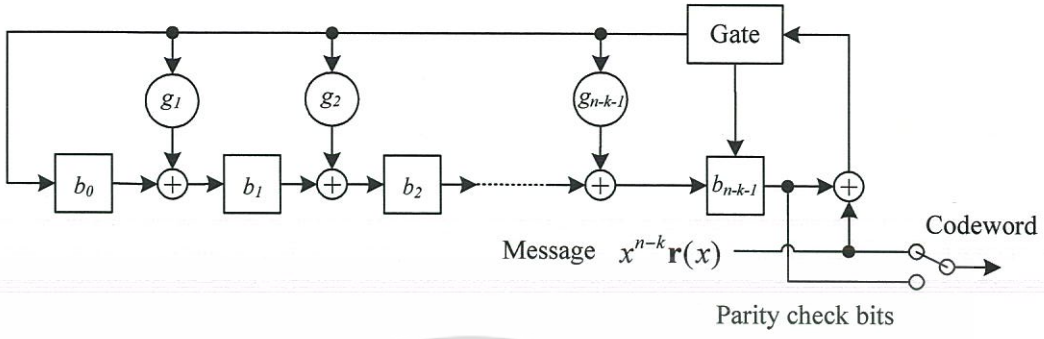
$$\mathbf{c}(x) = \mathbf{m}(x)\mathbf{g}(x) \tag{2.44}$$

จากสมการที่ (2.44) การเข้ารหัสที่ได้เป็นแบบไม่เป็นระบบ (Non-systematic)
ในการการเข้ารหัสเชิงระบบนั้นทำได้ดังสมการที่ (2.45)

$$\mathbf{c}(x) = \mathbf{r}(x) + x^{n-k}\mathbf{m}(x) \tag{2.45}$$

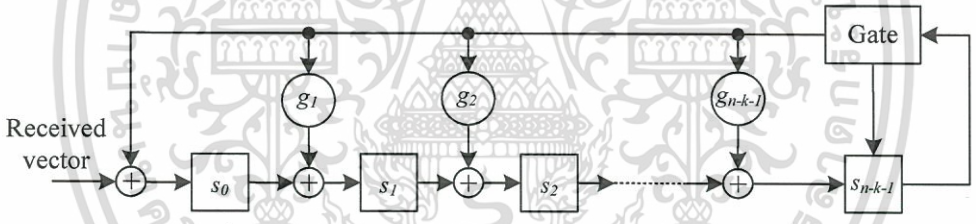
โดยที่ $\mathbf{r}(x) = \mathbf{m}(x) \bmod \mathbf{g}(x)$ และเรจิสเตอร์แบบเลื่อนจะคำนวณเฉพาะ $\mathbf{r}(x)$ เท่านั้น

ในส่วนของฮาร์ดแวร์ การเข้ารหัสไซคลิคสามารถนำเรจิสเตอร์แบบเลื่อนที่มีการป้อนกลับสร้างวงจรเข้ารหัสดังรูปที่ 2.4



รูปที่ 2.4 วงจรเข้ารหัสไซคลิก (n,k) โดยใช้เรจิสเตอร์แบบเลื่อน

การถอดรหัสซินโดรมสามารถนำเรจิสเตอร์แบบเลื่อนที่มีการป้อนกลับสร้างวงจรเข้ารหัสดังรูปที่ 2.5 ในการคำนวณหาซินโดรม $\mathbf{s}(x)$ เพื่อหาแพทเทิร์นของบิตผิดพลาดและนำไปแก้ไขความผิดพลาดของข้อมูลที่ได้รับ $\mathbf{r}(x)$



รูปที่ 2.5 วงจรถอดรหัสซินโดรมโดยใช้เรจิสเตอร์แบบเลื่อน

2.15 รหัสควอไซไซคลิค

รหัสควอไซไซคลิค (Quasi-cyclic codes) เป็นรหัสบล็อกเชิงเส้นชนิดหนึ่งที่มีคุณสมบัติการเลื่อนวนเช่นเดียวกับรหัสไซคลิก การเข้ารหัสของรหัสควอไซไซคลิคสามารถประยุกต์ใช้กับการเข้ารหัสแบบขนานได้ โดยเมทริกซ์กำเนิดของรหัสควอไซไซคลิคจะถูกแบ่งออกเป็นเมทริกซ์ย่อยขนาด $b\times b$ ซึ่งในแต่ละแถวจะถูกเลื่อนวนไปทางขวาหนึ่งครั้ง ดังนั้นรหัสควอไซไซคลิคจะมีเมทริกซ์กำเนิดในรูปของรหัสเชิงระบบดังนี้

$$\mathbf{G}_{qc,sys}=\begin{bmatrix}\mathbf{G}_0\\ \mathbf{G}_1\\ \vdots\\ \mathbf{G}_{c-1}\end{bmatrix}=\begin{bmatrix}\underbrace{\begin{matrix}\mathbf{G}_{0,0} & \mathbf{G}_{0,1} & \cdots & \mathbf{G}_{0,t-c-1}\\ \mathbf{G}_{1,0} & \mathbf{G}_{1,1} & \cdots & \mathbf{G}_{1,t-c-1}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{G}_{c-1,0} & \mathbf{G}_{c-1,1} & \cdots & \mathbf{G}_{c-1,t-c-1}\end{matrix}}_{\mathbf{I}_{cb}} & \underbrace{\begin{matrix}\mathbf{I} & \mathbf{O} & \cdots & \mathbf{O}\\ \mathbf{O} & \mathbf{I} & \cdots & \mathbf{O}\\ \vdots & \vdots & \ddots & \vdots\\ \mathbf{O} & \mathbf{O} & \cdots & \mathbf{I}\end{matrix}}_{\mathbf{P}}\end{bmatrix} \tag{2.46}$$

เมื่อ $\mathbf{I}$ คือเมทริกซ์เอกลักษณ์ที่มีขนาด $b \times b$, $\mathbf{O}$ คือเมทริกซ์ศูนย์ที่มีขนาด $b \times b$ และ $\mathbf{G}_{i,j}$ คือเมทริกซ์หมุนสลับตำแหน่งที่มีขนาด $b \times b$ $\mathbf{P}$ คือข้อมูลในส่วนพาริตี้ และ $\mathbf{I}_{cb}$ คือส่วนของข้อมูลที่ต้องการส่ง โดยให้ข้อมูลที่ต้องการส่งคือเวกเตอร์ $\mathbf{m}$

$$\begin{aligned}\mathbf{m} &= (\mathbf{m}_0, \mathbf{m}_1, ..., \mathbf{m}_{c-1}) \\ &= (m_0, m_1, ..., m_{cb-1})\end{aligned}$$

การเข้ารหัสเชิงระบบทำได้ดังสมการที่ (2.47)

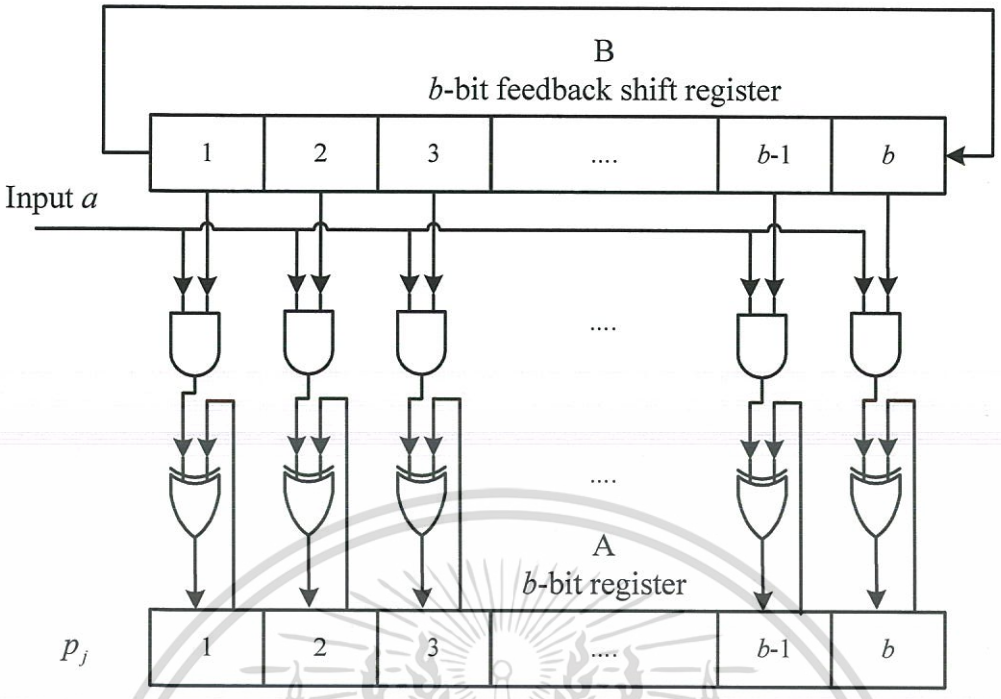
$$\mathbf{c} = \mathbf{mG} = \mathbf{m}_0\mathbf{G}_0 + \mathbf{m}_1\mathbf{G}_1 + \cdots + \mathbf{m}_{c-1}\mathbf{G}_{c-1} \tag{2.47}$$

$$\mathbf{c} = (\mathbf{p}_0, \mathbf{p}_1, \ldots, \mathbf{p}_{t-c}, \mathbf{m}_0, \mathbf{m}_1 \ldots, \mathbf{m}_{c-1}) \tag{2.48}$$

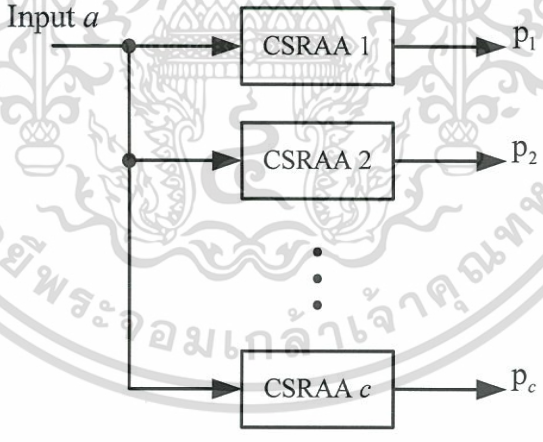
เมื่อ $\mathbf{p}$ คือข้อมูลในส่วนพาริตี้ของคำรหัส

$$\mathbf{p}_j = \mathbf{m}_0\mathbf{G}_{0,j} + \mathbf{m}_1\mathbf{G}_{1,j} + \cdots \mathbf{m}_{c-1}\mathbf{G}_{c-1,j} \tag{2.49}$$

การเข้ารหัสเชิงระบบของรหัสควอไซไซคลิคสามารถนำมาประยุกต์ใช้กับ Cyclic shift register-adder-accumulator (CSRAA) ได้โดยที่เมทริกซ์ $\mathbf{G}_{i,j}$ จะถูกเก็บไว้ในรีจีสเตอร์ B เมื่อบิตข้อมูล $\mathbf{m}$ ถูกนำเข้ามาก็จะถูกคูณด้วยเมทริกซ์ $\mathbf{G}_{i,j}$ โดยวงจรแอนด์เกต จากนั้นจึงถูกบวกกับเวกเตอร์ $\mathbf{p}_j$ ที่ได้จากการคำนวณก่อนหน้า ดังรูปที่ 2.6 ทั้งนี้บิตพาริตี้ทั้งหมดสามารถคำนวณหาได้ในเวลาเดียวกัน โดยใช้การเข้ารหัสแบบขนานดังรูปที่ 2.7 ซึ่งวงจรเข้ารหัสจะใช้ CSRAA จำนวน *t-c* ที่มีจำนวนฟลิปฟล็อปเท่ากับ $2(t-c)b$ และจำนวนแอนด์เกตและเอ็กคลูซีฟออร์เกตเท่ากับ $(t-c)/b$



รูปที่ 2.6 วงจรเข้ารหัส Cyclic shift register-adder-accumulator (CRRAA)



รูปที่ 2.7 วงจรเข้ารหัสแบบขนานโดยใช้ CRRAA

$$\mathbf{H} = \begin{bmatrix} \mathbf{A}_{0,0} & \mathbf{A}_{0,1} & \cdots & \mathbf{A}_{0,t-1} \\ \mathbf{A}_{1,0} & \mathbf{A}_{1,1} & \cdots & \mathbf{A}_{1,t-1} \\ \vdots & \vdots & \ddots & \vdots \\ \mathbf{A}_{t-c-1,0} & \mathbf{A}_{t-c-1,1} & \cdots & \mathbf{A}_{t-c-1,t-1} \end{bmatrix} \tag{2.50}$$

เมื่อ $\mathbf{A}_{i,j}$ คือเมทริกซ์หมุนสลับตำแหน่งที่มีขนาด $b \times b$ และเมทริกซ์ตรวจสอบพาริตี้ของรหัสควอไซไซคลิคเมื่อคูณด้วยทรานสโพสเมทริกซ์กำเนิดแบบเชิงระบบจะต้องมีค่าเป็นเมทริกซ์ศูนย์ ดังสมการ

$$\mathbf{H}\mathbf{G}_{qc,sys}^{\mathbf{T}} = [\mathbf{O}], \tag{2.51}$$

ในบทนี้ได้กล่าวถึงพื้นฐานทางคณิตศาสตร์และพื้นฐานรหัสบล็อกเชิงเส้น การเข้ารหัสและการถอดรหัสบล็อกเชิงเส้น ซึ่งเป็นพื้นฐานสำคัญในการเรียนรู้และออกแบบรหัสบล็อกที่มีประสิทธิภาพสูง เช่น รหัสแอลดีพีซี ซึ่งจะได้กล่าวถึงในบทต่อไป

บทที่ 3
รหัสแอลดีพีซี

รหัสความหนาแน่นพาริตี้ต่ำหรือรหัสแอลดีพีซี (Low-Density Parity-Check Codes: LDPC) เป็นรหัสบล็อกเชิงเส้นที่มีประสิทธิภาพสูงและมีการทำงานเข้าใกล้ขอบเขตของแชนนอนเมื่อใช้บล็อกขนาดใหญ่ในระบบสื่อสาร ซึ่งปัจจุบันรหัสแอลดีพีซีได้นำประยุกต์ใช้งานจริงในมาตรฐานของ IEEE เช่น IEEE 802.11n [2], IEEE 802.16 [3] เป็นต้น โดยในบทนี้จะกล่าวถึงความเป็นมาของรหัสแอลดีพีซี คุณสมบัติ ประเภท โครงสร้างของเมทริกซ์ตรวจสอบพาริตี้ วิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ รวมทั้งการเข้ารหัสและการถอดรหัส

3.1 ความเป็นมาของรหัสแอลดีพีซี

รหัสความหนาแน่นพาริตี้ต่ำหรือรหัสแอลดีพีซีได้คิดค้นครั้งแรกในปี ค.ศ.1960 ในงานวิจัยระดับปริญญาเอกของ R. Gallager ที่ Massachusetts Institute of Technology (MIT) [4] ประเทศสหรัฐอเมริกา ในงานวิจัยได้นำเสนอรหัสบล็อกเชิงเส้นชนิดหนึ่งซึ่งจำนวนเลขหนึ่งที่พบในเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ นั้นมีจำนวนน้อยเมื่อเทียบกับขนาดของเมทริกซ์ตรวจสอบพาริตี้ทั้งนี้เพื่อให้ระยะห่างต่ำสุดของรหัสมีค่าสูงและได้เสนอกระบวนการถอดรหัสแบบวนซ้ำเพื่อใช้กับรหัสชนิดนี้ แต่ช่วงเวลาดังกล่าวรหัสแอลดีพีซียังไม่ได้รับความสนใจเนื่องจากขีดความสามารถในการสร้างฮาร์ดแวร์ไม่สามารถรองรับความซับซ้อนของการถอดรหัสแอลดีพีซีได้ และในระยะเวลาเดียวกันนั้นได้มีการค้นพบรหัสบล็อกเชิงเส้นประเภทอื่น เช่น รหัสบีซีเอช (BCH codes) ที่เป็นแก้ไขข้อมูลผิดพลาดแบบบิตและรหัสรีด-โซโลมอน (Reed-Solomon Code) ที่เป็นแก้ไขข้อมูลผิดพลาดแบบสัญลักษณ์ ซึ่งเป็นมีรหัสที่เหมาะสมในการสร้างฮาร์ดแวร์ในช่วงเวลาดังกล่าวมากกว่า โดยรหัสบีซีเอชและรหัสรีดโซโลมอนได้ถูกนำไปประยุกต์ใช้จริงมาอย่างยาวนาน จนกระทั่งในปีในปี ค.ศ.1981 R.M. Tanner [5] ได้นำเสนอการใช้กราฟที่มีชื่อว่า Tanner Graph หรือ Bipartite Graph อธิบายความสัมพันธ์ของรหัสแอลดีพีซี ซึ่งกราฟที่ได้นี้สามารถประยุกต์ใช้ร่วมกับอัลกอริทึมแบบรวมผลคูณ (sum-product algorithm) หรือกระบวนการส่งผ่านความเชื่อมั่น (belief propagation algorithm) และจุดเปลี่ยนที่สำคัญของรหัสแก้ไขข้อมูลผิดพลาดที่ก้าวสู่เทคโนโลยีการสื่อสารระบบดิจิทัลในปัจจุบันเกิดขึ้นในปี ค.ศ. 1998 โดย C. Berrou, A. Glavieux และปัญญา ฐิติมัชฌิมา [6] ได้มีคิดค้นรหัสเทอร์โบ (Turbo Code) ซึ่งเป็นรหัสคอนโวลูชั่นและพบว่ามีสมรรถนะในการทำงานที่เข้าใกล้ลิมิตของแชนนอน ต่อมาในปี ค.ศ. 1990 ได้มีงานวิจัยของ D. J. C. MacKay [7] ที่ได้ศึกษารหัสแอลดีพีซีด้วยโครงสร้างแบบสุ่มพบว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานที่เข้าใกล้ขอบเขตของแชนนอนเช่นเดียวกัน อีกทั้งในงานวิจัยของ Richardson T.J. [8] ได้แสดงให้เห็นว่ารหัสแอลดีพีซีมีสมรรถนะการทำงานที่ดีกว่ารหัสเทอร์โบสำหรับบล็อกข้อมูลที่มีขนาดใหญ่ จากงานวิจัยต่าง ๆ ที่ถูกนำเสนอและตีพิมพ์ใน

บทความต่าง ๆ ทำให้รหัสแอลดีพีซีกลับมาได้รับความสนใจจากนักวิจัยทั่วโลกและมีจากงานวิจัยด้านรหัสแก้ไขความผิดพลาดต่าง ๆ จำนวนมากที่ได้รับการเผยแพร่ในปัจจุบันเกี่ยวข้องกับรหัสแอลดีพีซี นอกจากนี้สมรรถนะที่ได้ของรหัสแอลดีพีซีและความซับซ้อนในการถอดรหัสที่ต่ำกว่ารหัสเทอร์โบ เป็นผลให้รหัสแอลดีพีซีได้รับความนิยมในการนำมาประยุกต์ใช้งานในระบบสื่อสารและระบบบันทึกข้อมูลในปัจจุบัน

3.2 คุณสมบัติของรหัสแอลดีพีซี

รหัสแอลดีพีซีเป็นรหัสแก้ไขข้อมูลผิดพลาดแบบรหัสบล็อกเชิงเส้น โดยแต่ละแถวและหลักในเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ มีจำนวนของ “1” เป็นจำนวนน้อย รหัสแอลดีพีซีมีสองแบบด้วยกัน คือ รหัสแอลดีพีซีแบบคงที่และแบบไม่คงที่ โดยแบบคงที่จะมีเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}_{(n-k)\times k}$ เท่ากับ w_c ในแนวตั้งและเท่ากับ w_r ในแนวนอน โดย w_c คือจำนวน “1” ในแนวตั้งและ w_r คือจำนวน “1” ในแนวนอนของเมทริกซ์ตรวจสอบพาริตี้ รหัสแอลดีซีดั้งเดิมที่เสนอโดย R. Gallager [4] เป็นรหัสไบนารีแอลดีพีซีแบบคงที่ที่มีขนาดของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ ที่มีขนาดใหญ่มาก แต่ความหนาแน่นของ “1” ในเมทริกซ์มีจำนวนน้อย ความยาวของ n สามารถกำหนดได้เป็น (n, w_c, w_r) สำหรับรหัสแอลดีพีซีแบบคงที่จะได้ $(n-k)w_r = nw_c$ เมื่อ $w_c < w_r$ โดยปกติ $w_c \geq 3$ จะมีค่าระยะห่างต่ำสุด $d_{\min} \geq w_c + 1$ โดยทั่วไปในการออกแบบเมทริกซ์ตรวจสอบพาริตี้จะกำหนดให้ w_c มีค่าเป็น 3 หรือ 4

3.3 ประเภทของรหัสแอลดีพีซี

คุณลักษณะของเมทริกซ์ตรวจสอบพาริตี้ได้รับความนิยมในการใช้เป็นตัวบ่งชี้ประเภทของรหัสแอลดีพีซี ซึ่งรหัสแอลดีพีซีสามารถแบ่งได้เป็น 2 ประเภทหลัก ได้แก่

1) รหัสแอลดีพีซีแบบคงที่ (regular LDPC codes)
เมทริกซ์ตรวจสอบพาริตี้ขนาด $m \times n$ ของรหัสแอลดีพีซีแบบคงที่ จะมีเลขหนึ่งในแต่ละแถวอยู่เป็นจำนวนเท่ากับ w_c และจำนวนเลขหนึ่งในแต่ละหลักเป็น w_r หรือจำนวนเส้นที่เชื่อมต่อกับโหนดตรวจสอบในกราฟแทนเนอร์มีจำนวนเท่ากับ w_c และจำนวนเส้นที่เชื่อมต่อกับโหนดสัญลักษณ์เท่ากับ w_r โดยที่ $w_r << n$ และ $w_c << m$ ทั้งนี้อัตรารหัสสำหรับรหัสแอลดีพีซีแบบคงที่สามารถคำนวณได้จาก

$$R \geq 1 - \frac{m}{n} = 1 - \frac{w_r}{w_c} \tag{3.1}$$

2) รหัสแอลดีพีซีแบบไม่คงที่ (irregular LDPC codes)

T.Richardson [8] ได้นำเสนอรหัสแอลดีพีซีแบบไม่คงที่ในปี ค.ศ.2001 ซึ่งเมทริกซ์ตรวจสอบพาริตี้ที่มีจำนวนเลขหนึ่งอยู่ในแต่ละแถวและหลักเป็นจำนวนไม่คงที่ ดังนั้นการกำหนดลักษณะของรหัสจึงแสดงด้วยระดับการแจกแจง (Degree-distribution) สำหรับจำนวนเลขหนึ่งที่อยู่ในหลักและจำนวนเลขหนึ่งที่อยู่ในแถวดังสมการที่ (3.2) และ (3.3)

$$\lambda(X) = \sum_{i=1}^{w_r} \lambda_i X^{i-1} \tag{3.2}$$

$$\rho(X) = \sum_{i=1}^{w_c} \rho_i X^{i-1} \tag{3.3}$$

โดยที่

λ_i คือ สัดส่วนระหว่างผลรวมของจำนวนสมาชิกที่ไม่เป็นศูนย์ของทุกหลักที่มีน้ำหนัก i ของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ กับผลรวมของจำนวนสมาชิกทุกตัวที่ไม่เป็นศูนย์ของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ เมื่อ $\sum_{i=2}^{w_r} \lambda_i = 1$

ρ_i คือ สัดส่วนระหว่างผลรวมของจำนวนสมาชิกที่ไม่เป็นศูนย์ของทุกแถวที่มีน้ำหนัก i ของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ กับผลรวมของจำนวนสมาชิกทุกตัวที่ไม่เป็นศูนย์ของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ เมื่อ $\sum_{i=2}^{w_c} \rho_i = 1$

ในส่วนอัตรารหัสสำหรับรหัสแอลดีพีซีแบบไม่คงที่สามารถคำนวณได้จาก

$$R \geq 1 - \frac{m}{n} = 1 - \frac{w_r}{w_c} \tag{3.4}$$

3.4 กราฟแทนเนอร์

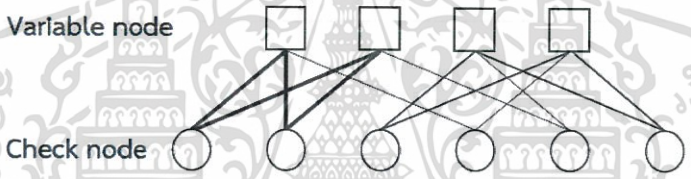
กราฟแทนเนอร์ (Tanner Graph) จัดว่าเป็นกราฟไบพาร์ไทต์ (Bipartite Graph) ชนิดหนึ่งที่ใช้อธิบายกระบวนการทำงานของรหัสแอลดีพีซี ซึ่งถือได้ว่าเป็นงานวิจัยที่มีบทบาทสำคัญในการนำทฤษฎีกราฟมาประยุกต์ใช้กับรหัสแก้ไขความผิดพลาด โดยกราฟแทนเนอร์ประกอบด้วยเส้นเชื่อม (Edge) กลุ่มโหนดจำนวน 2 กลุ่ม คือ โหนดสัญลักษณ์ (Variable node) เป็นตัวแทนของคำรหัส และโหนดตรวจสอบ (Check node) เป็นตัวแทนของเมทริกซ์พาริตี้ กลุ่มโหนดทั้งสองจะถูกเชื่อมเข้าด้วยกันเพื่อให้ได้ ความสัมพันธ์ของคำรหัสและเมทริกซ์ตรวจสอบพาริตี้ ดังรูปที่ 3.1 (ก) และ (ข)

วงรอบ (Cycle) หรือไซเคิลคือเส้นกราฟที่มีการเชื่อมต่อระหว่างโหนดบิตและโหนดตรวจสอบ และมีการเชื่อมต่อกับโหนดอื่นๆโดยมีโหนดเริ่มต้นและโหนดสิ้นสุดเป็นโหนดๆเดียวกัน

วงปิดรอบที่สั้นที่สุดของกราฟแทนเนอร์จะเรียกว่า “เกิรธ (Girth)” โดยเกิรธจะส่งผลถึงการลู่เข้าของคำตอบในการถอดรหัสแบบบวนซ้ำ จากรูปที่ 3.1 เส้นทึบที่แสดงเกิรธเท่ากับ 4 ในการออกแบบรหัสแอลพีซีต้องไม่ให้มีเกิรธ 4 อยู่เลย เนื่องจากเกิรธส่งผลต่อประสิทธิภาพในการถอดรหัสและทำให้คำตอบในการถอดรหัสแบบบวนซ้ำไม่ลู่เข้าหาคำตอบที่ถูกต้อง ดังนั้นเกิรธขั้นต่ำของรหัสแอลดีพีซีต้องมีเกิรธเท่ากับหรือมากกว่า 6 ในการออกแบบเมทริกซ์ตรวจสอบพาริตี้

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

(ก) เมทริกซ์ตรวจสอบพาริตี้



(ข) กราฟแทนเนอร์

รูปที่ 3.1 ความสัมพันธ์ระหว่างเมทริกซ์ตรวจสอบพาริตี้และกราฟแทนเนอร์

จาก [9] ได้แสดงความสัมพันธ์ระหว่างเกิรธและน้ำหนัก 1 ในแนวตั้ง (Column weight) กับระยะห่างต่ำสุด โดยระยะห่างต่ำสุดจะมีค่าเพิ่มขึ้นเมื่อเกิรธมีขนาดใหญ่ขึ้นหรือน้ำหนักแนวตั้งมีค่ามากขึ้น ดังสมการที่ (3.5)

$$d_{\min} \geq \begin{cases} 1 + w_c + w_c(w_c-1) + w_c(w_c-1)^2 + \cdots + w_c(w_c-1)^{(g-6)/4} & \text{for odd } g/2 \\ 1 + w_c + w_c(w_c-1) + w_c(w_c-1)^2 + \cdots + w_c(w_c-1)^{(g-8)/4} & \text{otherwise} \end{cases} \quad (3.5)$$

3.5 โครงสร้างของรหัสแอลดีพีซี

จากโครงสร้างรหัสแอลดีพีซีแบบคงที่ที่ R. Galager ได้นำเสนอไว้ในปี 1960 หลังจากนั้นในปี ค.ศ. 1998 David Mckey ได้เสนอโครงสร้างที่ใช้การสุ่มค่า นักวิจัยได้คิดค้นโครงสร้างแบบอื่นๆ เพื่อให้มีประสิทธิภาพสูงและง่ายต่อการนำประยุกต์ใช้งานจริง โดยส่วนใหญ่จะเป็นการออกแบบที่มีโครงสร้างที่แน่นอนหรือโครงสร้างที่ใช้การสุ่ม

3.5.1 รหัสอาร์เรย์

รหัสอาร์เรย์ (Array code) ได้ถูกนำเสนอในปี ค.ศ. 2000 โดย J.L. Fan [10] ซึ่งเมทริกซ์ตรวจสอบพาริตี้ของรหัสอาร์เรย์มีลักษณะเป็นโครงสร้างที่แน่นอน ทำให้ลดความซับซ้อนในการสร้างเมทริกซ์พาริตี้ นอกจากนี้ J. Fan ยังได้พิสูจน์ให้เห็นว่ารหัสอาร์เรย์ที่นำเสนอนี้ปราศจากไซเคิลขนาดเท่ากับ 4 ซึ่งส่งผลต่อสมรรถนะของอัลกอริทึมที่ใช้การถอดรหัสแอลดีพีซี ทั้งนี้เมทริกซ์ตรวจสอบพาริตี้ของรหัสอาร์เรย์จะมีขนาด $jp \times kp$ โดยที่จำนวนเต็ม j และ p ต้องมีค่าที่น้อยกว่าหรือเท่ากับจำนวนเฉพาะ p ตามสมการที่ (3.6)

$$\mathbf{I}=\begin{bmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{bmatrix}_{p\times p},\ \mathbf{P}_1=\begin{bmatrix}0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\end{bmatrix}_{p\times p},\ \mathbf{P}_2=\begin{bmatrix}0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\\1&0&0&0&0\\0&1&0&0&0\end{bmatrix}_{p\times p} \tag{3.6}$$

โดย $\mathbf{I}$ คือเมทริกซ์เอกลักษณ์ และ $\mathbf{P}$ คือเมทริกซ์หมุนสลับตำแหน่งโดยเลื่อนไปทางขวา (หรือทางซ้ายได้เช่นกัน) และเลขตัวเลขด้านล่างของ $\mathbf{P}$ คือค่าที่กำหนดการเลื่อนของ “1” ในเมทริกซ์หมุนสลับตำแหน่ง และ p คือขนาดของเมทริกซ์หมุนสลับตำแหน่ง จากสมการที่ (3.6) โครงสร้างของเมทริกซ์ตรวจสอบพาริตี้ของรหัสอาร์เรย์มีรูปแบบ ดังสมการที่ (3.7)

$$\mathbf{H}=\begin{bmatrix}\mathbf{I}&\mathbf{I}&\mathbf{I}&\cdots&\mathbf{I}\\\mathbf{I}&\mathbf{P}^{1}&\mathbf{P}^{2}&\cdots&\mathbf{P}^{k-1}\\\vdots&\vdots&\vdots&\ddots&\vdots\\\mathbf{I}&\mathbf{P}^{j-1}&\mathbf{P}^{j-1}&\cdots&\mathbf{P}^{k-1\cdot j-1}\end{bmatrix}_{jp\times kp} \tag{3.7}$$

โดย j คือจำนวนเมทริกซ์ย่อยในแนวนอน และ k คือจำนวนเมทริกซ์ย่อยในแนวตั้ง จากโครงสร้างของรหัสอารย์ในสมการที่ (3.6) สามารถหาค่าอัตรารหัสของการออกแบบ (Design rate) ซึ่งจะมีค่าเท่ากับอัตรารหัสที่ต้องการนำไปใช้งานจริง (Actual rate) ได้ดังนี้

$$R=1-\left(\frac{pj-j+1}{p^2}\right) \tag{3.8}$$

3.5.2 รหัสอาร์เรย์แบบปรับปรุง

งานวิจัยรหัสแอลดีพีซีแบบอาร์เรย์ในปี ค.ศ. 2000 ของ J. Fan ได้ถูกนำมาพัฒนาและได้ถูกนำเสนออีกครั้งในปี ค.ศ. 2002 โดย E. Eleftheriou [11] และเรียกวิธีการออกแบบดังกล่าวว่า รหัสอาร์เรย์แบบปรับปรุง (Modify array code) ซึ่งรหัสที่ได้นำเสนอนี้มีคุณลักษณะแบบไซคลิกทำให้การเข้ารหัสกระทำได้ง่ายโดยการใช้ชิฟท์รีจีสเตอร์ (shift register) ที่มีการป้อนกลับ และยังคงปราศจากไซเคิลขนาดเท่ากับ 4 ตามแบบรหัสอาร์เรย์ที่ได้นำเสนอไว้ โดยการออกแบบรหัสอาร์เรย์แบบปรับปรุงนี้สามารถทำได้โดยดัดแปลงรหัสอาร์เรย์ที่ได้นำเสนอไว้แล้วให้มีลักษณะเป็นเมทริกซ์เฉียง (diagonal matrix) ดังต่อไปนี้

$$\mathbf{H}=\begin{bmatrix} \mathbf{I} & \mathbf{I} & \mathbf{I} & \cdots & \mathbf{I} \\ \mathbf{0} & \mathbf{I} & \mathbf{P}^{1} & \cdots & \mathbf{P}^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{I} & \cdots & \mathbf{P}^{k-1\cdot j-1} \end{bmatrix}_{jp\times kp} \tag{3.9}$$

จากโครงสร้างของรหัสอารย์ในสมการที่ (3.9) สามารถหาค่าอัตรารหัสของการออกแบบและอัตรารหัสที่ต้องการนำไปใช้งานจริง หรือกล่าวคืออัตรารหัสของการออกแบบเท่ากับอัตรารหัสที่ต้องการนำไปใช้งานจริงได้ดังนี้

$$R=1-\left(\frac{pj-j+1}{p^{2}}\right) \tag{3.10}$$

3.5.3 รหัสควอไซไซคลิค

การนำรูปแบบของรหัสควอไซไซคลิคมาประยุกต์ใช้ในรหัสแอลดีพีซี โครงสร้างของเมทริกซ์ตรวจสอบพาริตี้ของรหัสควอไซไซคลิคมีรูปแบบดังสมการที่ (3.11)

$$\mathbf{H}=\begin{bmatrix} \mathbf{P}_{1,1} & \mathbf{P}_{1,2} & \mathbf{P}_{1,3} & \cdots & \mathbf{P}_{1,k-1} \\ \mathbf{P}_{2,1} & \mathbf{P}_{2,2} & \mathbf{P}_{2,3} & \cdots & \mathbf{P}_{2,k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \mathbf{P}_{j-1,1} & \mathbf{P}_{j-1,2} & \mathbf{P}_{j-1,3} & \cdots & \mathbf{P}_{j-1,k-1} \end{bmatrix}_{jp\times kp} \tag{3.11}$$

ปี ค.ศ. 2004 M. P. C. Fossorier [12] ได้เสนอบทความของรหัสควอไซไซคลิคแอลดีพีซีและได้แสดงผลว่ารหัสดังกล่าวสามารถสร้างเกิรธที่ขนาด 6, 8, 10 และ 12 จากการใช้คอมพิวเตอร์คำนวณค้นหารวมทั้งค่าโดยประมาณของระยะห่างต่ำสุด ในปีเดียวกันนั้น Tanner [13] เสนอวิธีการ

ออกแบบโดยใช้การออกแบบด้วยหมุนสลับตำแหน่ง ซึ่งสามารถใช้ในรหัสบล็อกและรหัสคอนโวลูชั่น โดยรูปแบบในการออกแบบสำหรับรหัสแอลดีพีซีแบบรหัสบล็อกเชิงเส้น มีรูปแบบดังสมการที่ (3.12)

$$\mathbf{H}=\begin{bmatrix} 1 & a & a^2 & \cdots & a^{k-1} \\ b & ab & a^2b & \cdots & a^{k-1}b \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b^{j-1} & ab^{j-1} & a^2b^{j-1} & \cdots & a^{k-1}b^{j-1} \end{bmatrix}_{jp\times kp} \tag{3.12}$$

โดยพารามิเตอร์ในการออกแบบของ Tanner จะกำหนดอิลิเมนต์ขึ้นมา 2 ค่า คือ a และ b โดยทั้งสองค่าคือจำนวนในการหมุนของเมทริกซ์หมุนสลับตำแหน่งมีค่าตั้งแต่ $1\le a,b<p$ ในปี ค.ศ 2014 Morteza Esmaeili [14] ได้เสนอวิธีการออกแบบโดยใช้ Cyclotomic coset โดยหลักการคือการคำนวณหาเซตร่วมที่มีสมาชิกไม่ซ้ำค่ามาต่อรวมกัน โดยหาจากสมการที่ (3.13)

$$C_s=(s,\rho s,\rho^2 s,...,\rho^{m-1}s) \tag{3.13}$$

<u>ตัวอย่างที่ 3.1</u> การออกแบบรหัสแอลดีพีซีบนโครงสร้างรหัสควอไซไซคลิคโดยใช้ Cyclotomic coset เมื่อกำหนดให้เมทริกซ์หมุนสลับตำแหน่งเท่ากับ $m=p=17$ และกำหนดอิลิเมนต์ ρ เท่ากับ 2 โดยวิธีการหา Cyclotomic coset ของชุดตัวเลขทั้งหมดจะหาได้จากสมการที่ (3.13) โดยกำหนดค่า s เริ่มต้นจาก 0 จะได้สมาชิกของเซตร่วมชุดแรกเป็น $C_0=\{0\}$ จากนั้นเพิ่มค่า s เพิ่มขึ้นทีละค่าโดยค่า s ค่าถัดไปมีค่าเป็น 1 จะได้เซตร่วมเป็น $C_1=\{1,2,4,8,16,15,13,9\}$ ต่อมาเพิ่มค่า s เป็น 2 แต่เนื่องจาก 2 เป็นสมาชิกในเซตร่วม C_1 แล้ว ดังนั้นค่า s ค่าถัดไปจึงมีค่าเป็น 3 ได้เซตร่วมเป็น $C_3=\{3,6,12,7,14,11,5,10\}$ และไม่ต้องหาเซตร่วมชุดถัดไปเนื่องจากสมาชิกของเซตร่วมทั้ง 3 ที่คำนวณหาได้นั้นมีสมาชิกครบทุกค่าแล้ว จากนั้นให้นำเซตร่วมทั้งหมดมาต่อรวมกันและใช้เป็นการกำหนดค่าของเมทริกซ์หมุนสลับตำแหน่งในแถวแรก $[C_0\ C_1\ C_3]$ จาก $C_0=\{0\}$ แทน 0 ในที่นี้คือเมทริกซ์เอกลักษณ์ที่มีขนาด $p\times p$ และให้เมทริกซ์ตรวจสอบพาริตี้ไม่มีเมทริกซ์เอกลักษณ์ ดังนั้นการกำหนดค่าของเมทริกซ์หมุนสลับตำแหน่งในแถวแรกของเมทริกซ์ตรวจสอบพาริตี้จะประกอบด้วย $[C_1\ C_3]$ ดังนั้นจะได้

$$\mathbf{H}_1=[1\ \ 2\ \ 4\ \ 8\ \ 16\ \ 15\ \ 13\ \ 9\ \ 3\ \ 6\ \ 12\ \ 7\ \ 14\ \ 11\ \ 5\ \ 10]$$

เมื่อได้เมทริกซ์หมุนสลับตำแหน่งทั้งหมดในแถวแรก ให้ทำการหาค่า $\mathbf{H}_2$ จากการกำหนดอิลิเมนต์ทำการคูณกับ $\mathbf{H}_1$ และมอดูโลด้วย p ดังนี้ ถ้ากำหนดให้อิลิเมนต์คือ b และให้ $b=9$

$$\mathbf{H}_2 = b \times \mathbf{H}_1 = 9 \times [1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 15 \quad 13 \quad 9 \quad 3 \quad 6 \quad 12 \quad 7 \quad 14 \quad 11 \quad 5 \quad 10] \bmod 17$$
$$\mathbf{H}_2 = [9 \quad 18 \quad 36 \quad 72 \quad 144 \quad 135 \quad 117 \quad 81 \quad 27 \quad 54 \quad 108 \quad 63 \quad 126 \quad 99 \quad 45 \quad 90] \bmod 17$$
$$\mathbf{H}_2 = [9 \quad 1 \quad 2 \quad 4 \quad 8 \quad 16 \quad 15 \quad 13 \quad 9 \quad 3 \quad 12 \quad 12 \quad 7 \quad 14 \quad 11 \quad 5]$$

จากนั้นคำนวณหาค่าในแถวต่าง ๆ ที่เหลือตามจำนวนน้ำหนัก 1 ในแนวตั้งจนครบดังนี้

$$\mathbf{H} = \begin{bmatrix} \mathbf{H}_1 \\ b\mathbf{H}_2 \\ \vdots \\ b^{j-1}\mathbf{H}_j \end{bmatrix}$$

สำหรับวิธีการออกแบบรหัสควอไซไซคลิคเพื่อให้ได้ขนาดของเกิรธที่ขนาดใหญ่และเป็นการออกแบบแบบที่เป็นลักษณะโครงสร้างและใช้คณิตศาสตร์ในการคำนวณ [15][16] ได้เสนอวิธีการออกแบบโดยใช้ One-Coincidence Sequence (OCS) เป็นวิธีการออกแบบโดยใช้โครงสร้างรหัสควอไซไซคลิคแอลดีพีซีเพื่อสร้างให้เมทริกซ์ตรวจสอบพาริตี้มีเกิรธขนาดตั้งแต่ 6 ขึ้นไป โดย Jen-Fa Huang [16] ได้เสนอวิธีการไว้ 3 แบบ คือ

1. Modified Welch–Costas (MWC) Sequences

$$y(u,v) = \begin{cases} \alpha\beta^{(m_u+n_v)} + \varphi \bmod p, & if \ 0 \le m_u \le p-2, 1 \le n_v \le p-1 \\ \varphi \bmod p, & if \ 0 \le m_u \le p-2, n_v = p \\ \varphi \bmod p, & if \ m_u = p-1, 1 \le n_v \le p-1 \end{cases} \quad (3.14)$$

เมื่อ p คือเลขจำนวนเฉพาะ และ $\alpha \in \{1,2,...,p-1\}$ และ $\beta \in \{0,1,2,...,p-1\}$

2. Quadratic Congruential Sequences

$$y(u,v) = [\alpha(m_u + n_v)^2 + \varphi_u + \varphi_v] \bmod p \quad (3.15)$$

เมื่อ $\alpha \in \{1,2,...,p-1\}$ และ $m_u, n_v, \varphi_u, \varphi_v \in \{0,1,2,...,p-1\}$

3. Shifted Prime (SP) Sequences

$$y(u,v) = m_u n_v + \varphi \bmod p \quad (3.16)$$

เมื่อ $m_u, n_v, \varphi \in \{0,1,2,...,p-1\}$

<u>ตัวอย่างที่ 3.2</u> การออกแบบรหัสควอไซไซคลิค (3, 5) โดยใช้ Modified Welch–Costas (MWC) Sequences ให้กำหนดค่าพารามิเตอร์ต่าง ๆ โดยกำหนดให้เมทริกซ์หมุนสลับตำแหน่ง $p=181$, $\alpha=1$, $\beta=2$, $\varphi=0$, $m_u=\{106,69,58\}$, $n_v=\{49,7,87,142,169\}$ โดย m_u และ n_v ในที่นี้มาจากการสุ่มค่า จากสมการ (3.14) ทำการคำนวณเพื่อเมทริกซ์ตรวจสอบพาริตี้ในทุกตำแหน่ง เช่น ตำแหน่งที่ $u=0, v=0$ จะได้ $y(0,0)=2^{(106+49)} \bmod 181=93$ ทำเช่นนี้ทุกตำแหน่ง ท้ายที่สุดเมทริกซ์ตรวจสอบพาริตี้จะมีค่าดังนี้

$$\mathbf{H}=\begin{bmatrix} \mathbf{I}(93) & \mathbf{I}(18) & \mathbf{I}(47) & \mathbf{I}(161) & \mathbf{I}(149) \\ \mathbf{I}(33) & \mathbf{I}(129) & \mathbf{I}(5) & \mathbf{I}(98) & \mathbf{I}(12) \\ \mathbf{I}(153) & \mathbf{I}(88) & \mathbf{I}(89) & \mathbf{I}(43) & \mathbf{I}(105) \end{bmatrix}$$

โดย $\mathbf{I}(x)$ คือเมทริกซ์เอกลักษณ์ที่มีเลื่อนข้อมูลไปทางขวา x ครั้ง

<u>ตัวอย่างที่ 3.3</u> การออกแบบรหัสควอไซไซคลิค (3, 5) โดยใช้ Quadratic Congruential Sequences ให้กำหนดค่าพารามิเตอร์ต่าง ๆ โดยกำหนดให้เมทริกซ์หมุนสลับตำแหน่ง $p=31$, $\alpha=1$, $\beta=2$, $\varphi_u=0$, $\varphi_v=0$, $m_u=\{18,14,15\}$ และ $n_v=\{23,11,25,24,17\}$ โดย m_u และ n_v ในที่นี้มาจากการสุ่มค่า จากสมการ (3.15) ทำการคำนวณเพื่อเมทริกซ์ตรวจสอบพาริตี้ในทุกตำแหน่ง เช่น ตำแหน่งที่ $u=0, v=0$ จะได้ $y(0,0)=[1(18+23)^2+0+0] \bmod 31=7$ ทำเช่นนี้ทุกตำแหน่ง จะได้เมทริกซ์ตรวจสอบพาริตี้ดังนี้

$$\mathbf{H}=\begin{bmatrix} \mathbf{I}(7) & \mathbf{I}(4) & \mathbf{I}(20) & \mathbf{I}(28) & \mathbf{I}(16) \\ \mathbf{I}(5) & \mathbf{I}(5) & \mathbf{I}(2) & \mathbf{I}(18) & \mathbf{I}(0) \\ \mathbf{I}(18) & \mathbf{I}(25) & \mathbf{I}(19) & \mathbf{I}(2) & \mathbf{I}(1) \end{bmatrix}$$

<u>ตัวอย่างที่ 3.4</u> การออกแบบรหัสควอไซไซคลิค (3, 5) โดยการออกแบบด้วยวิธี Shifted Prime (SP) Sequences ให้กำหนดค่าพารามิเตอร์ต่าง ๆ โดยกำหนดให้เมทริกซ์หมุนสลับตำแหน่ง $p=31$, $\varphi=0$, $m_u=\{0,1,3\}$ และ $n_v=\{0,1,2,5,8\}$ โดย m_u และ n_v ได้มาจาก [16] ซึ่งเป็นลำดับที่ทำให้เกิรธ 8 จากนั้นทำการคำนวณตามสมการที่ (3.16) เช่น ตำแหน่งที่ $u=0, v=0$ จะได้ $y(0,0)=[(0\times 0)+0] \bmod 31=0$ และทำการคำนวณในตำแหน่งที่เหลือทั้งหมดจะได้เมทริกซ์ตรวจสอบพาริตี้ที่มีขนาดเกิรธเท่ากับ 8 ดังนี้

$$\mathbf{H}=\begin{bmatrix} \mathbf{I}(0) & \mathbf{I}(0) & \mathbf{I}(0) & \mathbf{I}(0) & \mathbf{I}(0) \\ \mathbf{I}(0) & \mathbf{I}(1) & \mathbf{I}(2) & \mathbf{I}(5) & \mathbf{I}(8) \\ \mathbf{I}(0) & \mathbf{I}(3) & \mathbf{I}(6) & \mathbf{I}(15) & \mathbf{I}(24) \end{bmatrix}$$

จากตัวอย่างที่ได้แสดงวิธีการออกแบบจะเห็นได้ว่าพารามิเตอร์ที่สำคัญในการออกแบบคือลำดับตัวเลขของ m_u และ n_v โดยลำดับตัวเลขนี้สามารถที่กำหนดค่าเพื่อสร้างให้เมทริกซ์ตรวจสอบพาริตี้สร้างเกิรธขนาดมากกว่า 6 ได้ด้วยการใช้อัลกอริทึมในการค้นหาที่เรียกว่าสมการไซเคิลโกเวินนิ่ง (Cycle-governing equations หรือ CEG) และบทความนี้ได้สรุปตารางของลำดับตัวเลขเพื่อสร้างขนาดของเกิรธเท่ากับ 6, 8, 10 และ 12 แต่ทั้งนี้เกิรธที่ได้จะขึ้นอยู่กับอัตรารหัสและขนาดของเมทริกซ์หมุนสลับตำแหน่ง

จะเห็นได้ว่าวิธีการออกแบบรหัสแอลดีพีซีโดยใช้โครงสร้างควอไซไซคลิคเป็นรหัสที่ได้รับความนิยมและมีนักวิจัยได้เสนอวิธีการออกแบบไว้หลายรูปแบบ ทั้งนี้เนื่องจากเป็นที่ออกแบบง่ายและเหมาะสมในการนำไปสร้างฮาร์ดแวร์ จากที่ได้กล่าวมาเป็นเพียงวิธีการออกแบบบนโครงสร้างรหัสควอไซไซคลิคแอลดีพีซีเพียงบางส่วนเท่านั้น ยังมีบทความอีกจำนวนมากที่ไม่ได้กล่าวถึงซึ่งสามารถค้นคว้าเติมได้อีกมากมาย

ในส่วนของอัตรารหัสในการออกแบบและอัตรารหัสที่ต้องการนำไปใช้งานจริงของรหัสควอไซไซคลิคจะไม่เท่ากัน การหาค่าอัตราในการใช้งานจริงจะขึ้นอยู่กับขนาดของเมทริกซ์กำเนิด $\mathbf{G}$ หรือขึ้นอยู่กับข้อมูลที่ต้องส่งต่อข้อมูลที่ถูกเข้ารหัส

3.5.4 รหัสเรขาคณิตยูคลิด

เรขาคณิตขอบเขตจำกัด (Finite geometries) เช่นเรขาคณิตยูคลิด (Euclidean geometries) และเรขาคณิตเชิงภาพฉาย (Projective geometries) เป็นเครื่องมือที่มีประสิทธิภาพทางคณิตศาสตร์ที่ใช้ในการแก้ไขรหัสผิดพลาด Y. Kou [17][18][19] พิสูจน์ให้เห็นว่าเรขาคณิตขอบเขตจำกัดสามารถนำไปใช้ในการออกแบบรหัสแอลดีพีซีและมีประสิทธิภาพที่เข้าใกล้ทฤษฎีขอบเขตของแชนนอล เมื่อใช้การถอดรหัสวนซ้ำ โดยรหัสเหล่านี้เรียกว่ารหัสแอลดีพีซีเรขาคณิตขอบเขตจำกัด (Finite geometry LDPC) รูปแบบของรหัสแอลดีพีซีที่ถูกสร้างขึ้นจากพีชคณิตโดยพารามิเตอร์ในการสร้างเมทริกซ์ตรวจสอบพาริตี้โดยใช้เรขาคณิตยูคลิดกำหนดได้ดังตารางที่ 3.1

ตารางที่ 3.1 พารามิเตอร์ในการออกแบบรหัสเรขาคณิตยูคลิด

ความยาว (length)	$n = 2^{2s} - 1$
จำนวนบิตพาริตี้	$n - k = 3^s - 1$
Minimum distance	$d_{\min} = 2^s + 1$
Row weight	$\rho = 2^s$
Column weight	$\gamma = 2^s$

จากพารามิเตอร์ที่แสดงในตารางที่ 3.1 วิธีการออกแบบรหัสแอลดีพีซีแบบเรขาคณิตยูคลิดดังตัวอย่างต่อไปนี้

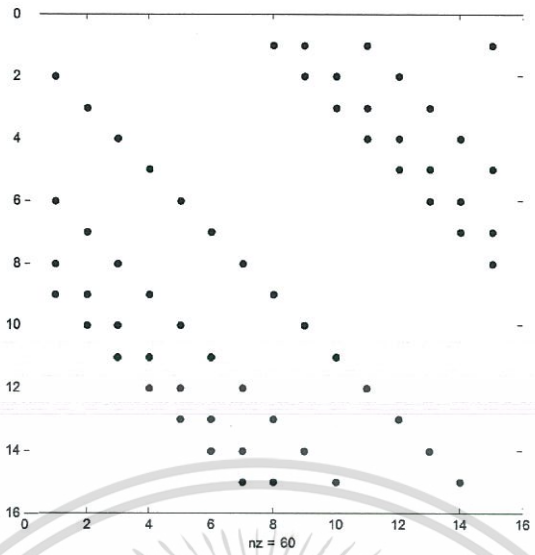
<u>ตัวอย่างที่ 3.5</u> การออกแบบ $EG(2,2^2)$ บน $GF(2^2)$ จากตัวอย่างที่ 2.1 ในบทที่ 2 คำนวณหาจุดทั้งหมด $n=16$ จุด แต่ละเส้นประกอบด้วยจุด 4 จุด เมื่อพิจารณา $GF(2^4)$ มีพหุนามตั้งต้น (Primitive polynomial) มีค่าเป็น $1+X+X^4$ บน $GF(2)$ กำหนดให้ α เป็นอิลิเมนต์ตั้งต้น (Primitive element) ของ $GF(2^4)$ และกำหนดให้ $\beta=\alpha^5$

$$GF(2^2)=\{0,\beta^0=1,\beta=\alpha^5,\beta^2=\alpha^{10}\}$$

จากสมการที่ (2.4) และสมการที่ (2.5) ในบทที่ 2 จะได้

$$L_0=\{\beta_1\alpha\}=\{0,\alpha,\alpha^6,\alpha^{11}\}$$
$$L_1=\{1+\beta_1\alpha\}=\{1,\alpha^4,\alpha^{12},\alpha^{13}\}$$
$$L_2=\{\alpha^5+\beta_1\alpha\}=\{\alpha^2,\alpha^3,\alpha^5,\alpha^9\}$$
$$L_3=\{\alpha^{10}+\beta_1\alpha\}=\{\alpha^8,\alpha^7,\alpha^{10},\alpha^{14}\}$$

ให้คำนวณหาเส้นที่ไม่ผ่านจุดกำเนิด (จุดที่มีค่าเป็น “0”) ซึ่งจะเส้นทั้งหมด 15 เส้น หรือใช้อีกวิธีหนึ่งเลือกเส้นเพียงเส้นเดียวและทำการไซคลิค (Cyclic) วิธีการคือเลือกเส้น 1 เส้นโดยไม่เลือกเส้นที่อยู่บนจุดกำเนิด (จากตัวอย่างไม่เลือก L_0 เนื่องจากมีจุด “0” อยู่ในเส้น) จากค่า L_0 ถึง L_3 ในตัวอย่างนี้เลือกเส้นที่อยู่บนจุด α^{14} คือ L_3 ต่อจากนั้นให้วางตำแหน่งของ “1” ในแถวแรกของเมทริกซ์ตรวจสอบพาริตี้ เช่น $L_3=\{\alpha^8,\alpha^7,\alpha^{10},\alpha^{14}\}$ พิจารณาเลขกำลังกำลังของ α คือดัชนีในการตำแหน่งของ “1” โดยให้เลขกำลังกำลังของ α บวกด้วย 1 ดังนั้นจะได้หลักที่ 8,9,11 และ 15 ในแถวแรกมีค่าเป็น “1” ส่วนหลักอื่นๆให้มีค่าเป็น “0” จากนั้นให้เลื่อนข้อมูลในแถวแรกไปทางขวาทีละ 1 ครั้งในแถวที่สองจนถึงแถวสุดท้ายจนครบจำนวนเส้นทั้งหมด 15 เส้น จะได้เมทริกซ์ตรวจสอบพาริตี้ดังรูปที่ 3.2 โดยจุดแทนค่า “1” ในเมทริกซ์



รูปที่ 3.2 เมทริกซ์ตรวจสอบพาริตี้ที่ออกแบบโดยโครงสร้างรหัสเรขาคณิตยูคลิด

3.5.5 รหัสเรขาคณิตเชิงภาพฉาย

รหัสเรขาคณิตเชิงภาพฉาย (Projective Geomety) เป็นการใช้หลักการทางคณิตศาสตร์ในการออกแบบรหัสแอลดีพีซีด้วยวิธีการนี้จะกำหนดจุด 2 จุดเป็นจุดเริ่มต้น วิธีการนี้ถูกเสนอโดย Y. Kou [17][18][19] ซึ่งอยู่ในบทความเดียวกันกับรหัสเรขาคณิตยูคลิด โดยค่าพารามิเตอร์ในการสร้างเมทริกซ์ตรวจสอบพาริตี้โดยใช้เรขาคณิตเชิงภาพฉายกำหนดได้ดังตารางที่ 3.2

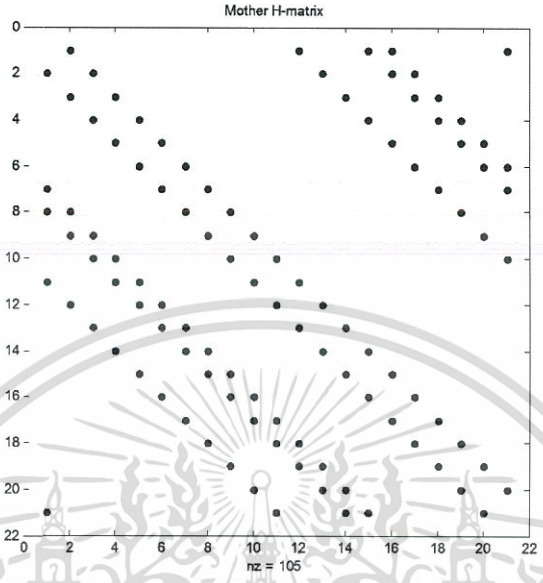
ตารางที่ 3.2 พารามิเตอร์ในการออกแบบรหัสเรขาคณิตเชิงภาพฉาย

ความยาว (length)	$n = 2^{2s} + 2^s + 1$
จำนวนบิตพาริตี้	$n - k = 3^s + 1$
ระยะห่างต่ำสุด (Minimum distance)	$d_{\min} = 2^s + 2$
น้ำหนัก 1 ในแนวนอน (Row weight)	$\rho = 2^s + 1$
น้ำหนัก 1 ในแนวตั้ง (Column weight)	$\gamma = 2^s + 1$

จากพารามิเตอร์ที่แสดงในตารางที่ 3.2 วิธีการออกแบบรหัสแอลดีพีซีแบบเรขาคณิตเชิงภาพฉายดังตัวอย่างต่อไปนี้

ตัวอย่างที่ 3.6 การออกแบบ $PG(2,2^2)$ บน $GF(64)$ จากตัวอย่างที่ 2.2 ในบทที่ 2 คำนวณหาจุดทั้งหมด $n = 21$ จุด โดย α เป็นพหุนามของ $GF(64)$ ให้ $\beta = \alpha^{21}$ และฟิลด์ย่อย $GF(2^2) = \{0, 1, \beta, \beta^2\}$ เส้นที่ผ่านจุด 2 จุด ระหว่างจุด (α) และ (α^{20}) มีจุดร่วมในเส้นเดียวกัน

คือนี้ $\{(\alpha),(\alpha^{11}),(\alpha^{14}),(\alpha^{15}),(\alpha^{20})\}$ เป็นจุดทั้งหมดของเส้น $PG(2,2^2)$ หลังจากนั้นให้ทำการหาเส้นที่ผ่านจุดทั้งหมดและจะได้เส้นทั้งหมด n เส้น หรือใช้วิธีการไซคลิค จะได้เมทริกซ์ตรวจสอบพาริตี้ดังรูปที่ 3.3 โดยจุดแทนค่า “1” ในเมทริกซ์



รูปที่ 3.3 เมทริกซ์ตรวจสอบพาริตี้ที่ออกแบบโดยโครงสร้างรหัสเรขาคณิตเชิงภาพฉาย

3.5.6 รหัสบล็อกไม่สมบูรณ์แบบสมดุล

รหัสบล็อกไม่สมบูรณ์แบบสมดุล (Balance Incomplete Block Design) หรือเรียกโดยย่อว่า บีไอบีดี (BIBD) [20][21] สำหรับการออกแบบเมทริกซ์ตรวจสอบพาริตี้โดยใช้การออกแบบบล็อกไม่สมบูรณ์แบบสมดุลในหัวข้อนี้เป็นวิธีการออกแบบจาก [21] โดยมีวิธีการอยู่ 2 แบบ เรียกว่า คลาสหนึ่ง (Class I) และ คลาสสอง (Class II) โดยรหัสการออกแบบบล็อกไม่สมบูรณ์แบบสมดุลคลาสหนึ่ง (BIBD Class-I) เป็นการออกแบบที่น้ำหนัก 1 ในแนวตั้งมีค่าเท่า 4 หรือ $j=4$ โดยวิธีการในการออกแบบจะทำการหาตำแหน่งเพื่อวางตำแหน่งของ “1” ในหลักแรก จากนั้นจะเลื่อนข้อมูลจากหลักแรก 1 ไปยังหลักถัดไป โดยจะเลื่อนข้อมูลลงทีละครั้งในแต่ละหลักจนครบบล็อก โดยใน 1 บล็อกคือเมทริกซ์จัตุรัส (Square matrix) หรือก็คือเมทริกซ์ตรวจสอบพาริตี้แบบไซคลิค จากนั้นให้ออกแบบด้วยวิธีการดังกล่าวกับบล็อกถัดไป โดยการหาตำแหน่งเพื่อวางตำแหน่งของ “1” ในหลักแรกให่คำนวณตามสมการดังต่อไปนี้ กำหนดให้ t เป็นเลขจำนวนเต็มบวก และ $12t+1$ เป็นเลขจำนวนเฉพาะใน $GF(12t+1)=\{0,1,....,12t\}$ ให้อิลิเมนต์เบื้องต้น (Primitive element) ของ $GF(12t+1)$ การคำนวณหาค่าอิลิเมนต์เบื้องต้น α ดังสมการที่ (3.10)

$$\alpha^{4t}-1=\alpha^{c} \tag{3.17}$$

เมื่อ c เป็นค่าเลขคี่จำนวนเต็มบวก และค่ามีน้อยกว่า $12t+1$ จากสนามจำกัด $GF(12t+1)$ และการคำนวณหาตำแหน่งในบล็อกแรกสามารถหาได้จากสมการที่ (3.18) และในส่วนของบล็อกอื่นๆหาได้จากสมการที่ (3.19)

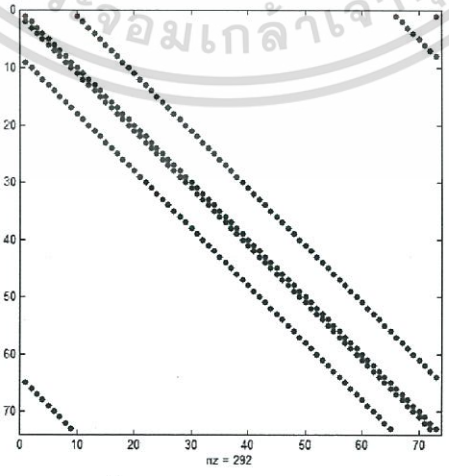
$$B_{i,0} = \{\alpha^{-\infty}, \alpha^{2i}, \alpha^{2i+4t}, \alpha^{2i+8t}\} \tag{3.18}$$

เมื่อ $0 \le i < t$

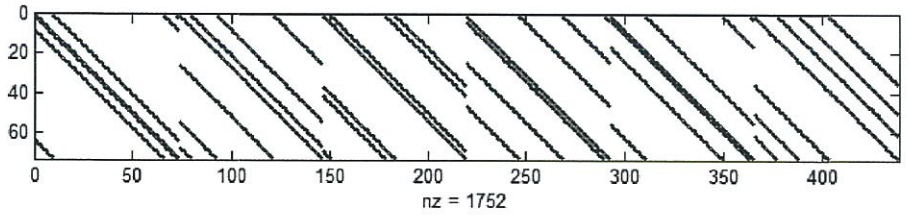
$$B_{i,j} = \{j+\alpha^{-\infty}, j+\alpha^{2i}, j+\alpha^{2i+4t}, j+\alpha^{2i+8t}\} \tag{3.19}$$

โดยที่ $0 \le j \le 12t$

ตัวอย่างที่ 3.7 กำหนดให้ $t=6$ จะได้ $12t+1=(12\times 6)+1=73$ ซึ่งเป็นเลขจำนวนเฉพาะ ดังนั้นจะอยู่ใน $GF(73)=\{0,1,2,...,72\}$ จากนั้นทำการคำนวณหาค่า α และ c จากสมการที่ (3.17) จะได้ค่า $\alpha=5$ และ $c=33$ ต่อจากนั้นทำการคำนวณหาค่าการวางตำแหน่ง “1” ในหลักแรกของบล็อกแรกโดยใช้สมการที่ (3.18) โดยบล็อกแรกจะให้ $i=0$ จะได้ $B_{0,0}=\{0,\alpha^{2\cdot 0},\alpha^{2\cdot 0+4\cdot 6},\alpha^{2\cdot 0+8\cdot 6}\}$ และแทนค่า $\alpha=5$ จะได้ $B_{0,0}=\{0,1,5^{24},5^{48}\}$ และเนื่องจากการออกแบบทำบน $GF(73)$ ดังนั้นจะได้ $B_{0,0}=\{0,1,8,64\}$ เมื่อหาค่าตำแหน่งการวาง “1” ในหลักแรกของบล็อกแรกแล้ว ให้ทำด้วยวิธีการเดียวกันนี้จนครบจำนวนตามจำนวน t หลัก โดยทำการคำนวณคำนวณหาค่าการวางตำแหน่ง “1” ในหลักถัดไปตามสามการที่ (3.19) เพื่อคำนวณหาค่า $B_{0,1}=\{1,2,9,65\}$, $B_{0,2}=\{2,3,10,66\}$,..., $B_{0,72}=\{72,0,7,63\}$ ตามลำดับ หรือสามารถอธิบายได้โดยง่ายคือหาตำแหน่งการวาง “1” ในหลักแรกจากนั้นเลื่อนข้อมูลลงทีละครั้งในหลักถัดๆไป รูปแบบของบล็อกแรกดังรูปที่ 3.4



รูปที่ 3.4 เมทริกซ์ตรวจสอบพาริตี้บล็อกแรกของรหัสบล็อกไม่สมบูรณ์แบบสมดุลคลาส I



รูปที่ 3.5 เมทริกซ์ตรวจสอบพาริตี้ที่ออกแบบโดยโครงสร้างรหัสบล็อกไม่สมบูรณ์แบบสมดุลคลาส I

รหัสการออกแบบบล็อกไม่สมบูรณ์แบบสมดุลคลาสสอง (BIBD Class-II) เป็นการออกแบบที่กำหนดให้ น้ำหนัก 1 ในแนวตั้งมีค่าเท่า 5 หรือ $j=5$ ซึ่งการออกแบบจะเหมือนกันกับ กำหนดให้ Class-I BIBD คือกำหนดให้ t เป็นเลขจำนวนเต็มบวก แต่จะใช้ $20t+1$ เป็นเลขจำนวนเฉพาะ

$$\alpha^{4t}-1=\alpha^{c} \tag{3.20}$$

เมื่อ c เป็นค่าเลขคี่จำนวนเต็มบวก และค่ามีน้อยกว่า $20t+1$ จากสนามจำกัด $GF(20t+1)$ และการคำนวณหาตำแหน่งในบล็อกแรกสามารถหาได้จากสมการที่ (3.21) และในส่วนของบล็อกอื่นๆหาได้จากสมการที่ (3.22)

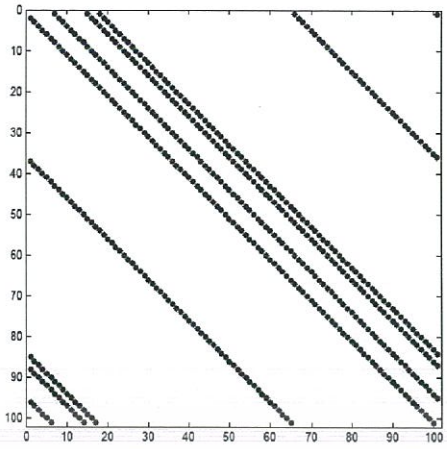
$$B_{i,0}=\{\alpha^{2i},\alpha^{2i+4t},\alpha^{2i+8t},\alpha^{2i+12t},\alpha^{2i+16t}\} \tag{3.21}$$

เมื่อ $0\le i<t$

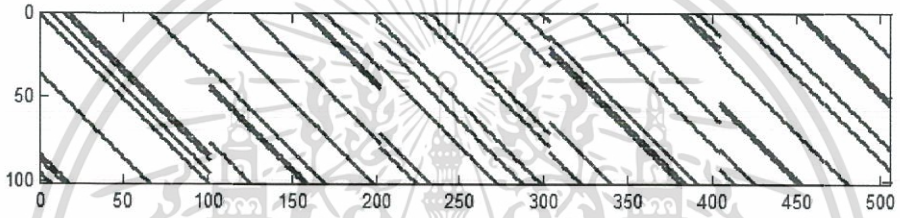
$$B_{i,j}=\{j+\alpha^{-\infty},j+\alpha^{2i},j+\alpha^{2i+4t},j+\alpha^{2i+8t}\} \tag{3.22}$$

โดยที่ $0\le j\le 20t$

<u>ตัวอย่างที่ 3.8</u> กำหนดให้ t=5 จะได้ $20t+1=(12\times 5)+1=61$ ซึ่งค่าที่ได้เป็นเลขจำนวนเฉพาะ จากนั้นคำนวณหาค่า α และ c จากสมการที่ (3.20) ได้ $\alpha=2$ และ $c=74$ และจากสมการที่ (3.21) ได้ $B_{0,0}=\{0,\alpha^{35},\alpha^{83},\alpha^{86},\alpha^{94}\}$ และจากสมการที่ (3.22) ได้ $B_{0,1}=\{\alpha^{3},\alpha^{32},\alpha^{42},\alpha^{44},\alpha^{76}\}$,



รูปที่ 3.6 เมทริกซ์ตรวจสอบพาริตี้บล็อกแรกของรหัสบล็อกไม่สมบูรณ์แบบสมดุลคลาส II



รูปที่ 3.7 เมทริกซ์ตรวจสอบพาริตี้ที่ออกแบบโดยโครงสร้างรหัสบล็อกไม่สมบูรณ์แบบสมดุลคลาส II

3.5.7 อัลกอริทึมพีอีจี

ความยาวของวงรอบในกราฟแทนเนอร์ส่งผลโดยตรงต่อสมรรถนะของการถอดรหัสแอลดีพีซีเมื่อจำนวนรอบในการถอดรหัสเพิ่มมากขึ้น ดังนั้นในปี 2001 X. Y. Hu [22] จึงได้นำเสนออัลกอริทึมในการสร้างกราฟแทนเนอร์เพื่อให้ความยาวของไซเคิลนั้นมากที่สุดเท่าที่ทำได้โดยได้นิยามโลคอลเกิรธ (Local girth) ของแต่ละโหนดสัญลักษณ์ ว่าเป็นระยะทางที่สั้นที่สุดในการเดินทางจากโหนดสัญลักษณ์ใดๆ ไปและกลับมายังโหนดสัญลักษณ์เดิม จากแผนภาพแสดงการเส้นทางจากโหนดสัญลักษณ์ในรูปที่ 3.8 แสดงให้เห็นถึงการขยายเส้นทางเพื่อให้ได้เกิรธ หากกิ่งก้านสาขามีการขยายลงไประดับที่มากวงรอบหรือโลคอลเกิรธที่ได้จะมีขนาดมากตาม โดยอัลกอริทึมพีอีจี (PEG algorithm) จะค่อยๆ สร้างเส้นเชื่อมจากโหนดสัญลักษณ์ที่ 1 ไปยังโหนดสัญลักษณ์ที่ n ซึ่งการสร้างเส้นเชื่อมในแต่ละครั้งนั้นจะต้องทำให้เกิดโลคอลเกิรธที่มากที่สุด วิธีการสร้างเมทริกซ์ตรวจสอบพาริตี้สามารถเขียนโปรแกรมได้ดังนี้

อัลกอริทึมพีอีจี

for $i = 0$ *to* n-1 *do*

for $k = 0$ *to* d_v -1 *do*

if $k = 0$

เลือกโหนดตรวจสอบที่มีจำนวนเลขหนึ่งในแถวที่น้อยที่สุด

else

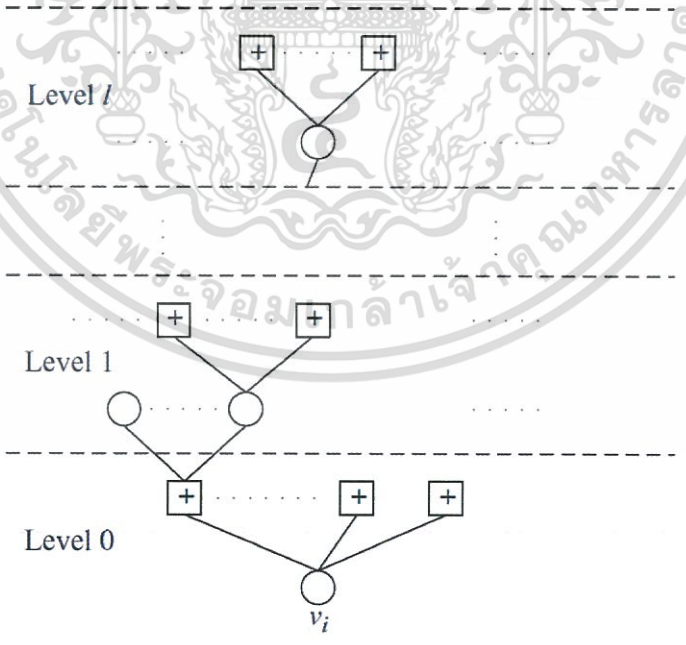
ทำการขยายกิ่งก้านสาขาไปเรื่อยจนกระทั่งถึง depth ที่ l แล้วทำการเลือกโหนดตรวจสอบที่อยู่ใน depth ที่ l (จะทำให้เกิดโลคอลเกิรธขนาด 2(l +2))

<u>หมายเหตุ</u> ในช่วงแรกๆ การขยายกิ่งก้านสาขาจะไม่สามารถไปถึงทุกโหนดตรวจสอบในที่นี้ให้เลือกโหนดตรวจสอบที่ขยายไปไม่ถึง (ในกรณีนี้จะไม่ทำให้เกิดโลคอลเกิรธ)

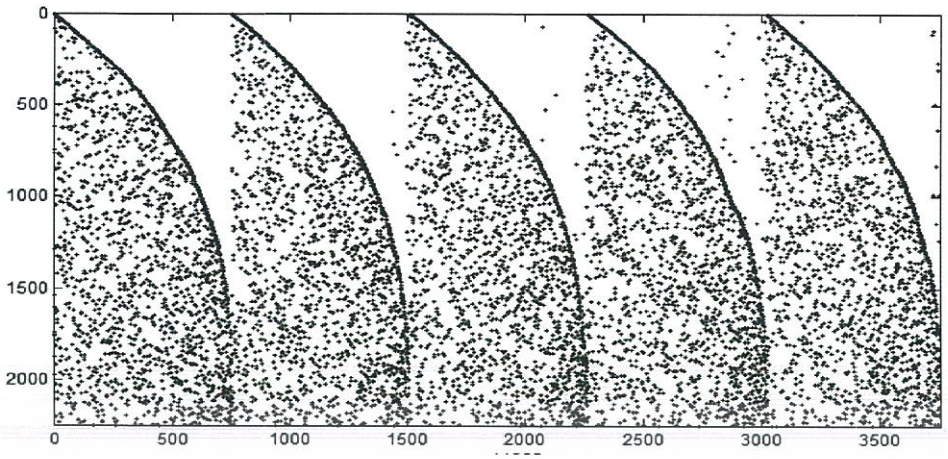
end

end

end



รูปที่ 3.8 แผนภาพแสดงการเส้นทางจากโหนดสัญลักษณ์



รูปที่ 3.9 เมทริกซ์ตรวจสอบพาริตี้ที่ออกแบบโดยโครงสร้างของอัลกอริทึมพีอีจี

3.6 การเข้ารหัสและถอดรหัสไบนารีแอลดีพีซี

การเข้ารหัสแอลดีพีซีทำได้จากการหาเมทริกซ์กำเนิด $\mathbf{G}$ จากเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}$ โดยคำรหัสสามารถแบ่งพาติชั่น (Partition) ได้ดังสมการที่ (3.23)

$$\mathbf{c} = [\mathbf{b} : \mathbf{m}] \tag{3.23}$$

โดย $\mathbf{m}$ คือข้อความอินพุทมีขนาด $1 \times k$ และ b คือบิตพาริตี้มีขนาด $1 \times (n-k)$ และทรานสโพสเมทริกซ์ตรวจสอบพาริตี้สามารถแบ่งพาติชั่นได้ดังสมการที่ (3.24)

$$\mathbf{H} = [\mathbf{H}_1 : \mathbf{H}_2] \tag{3.24}$$

เมื่อ $\mathbf{H}_1$ คือเมทริกซ์จัตุรัสมีขนาด $(n-k)\times(n-k)$ และ $\mathbf{H}_2$ คือเมทริกซ์สี่เหลี่ยมผืนผ้ามีขนาด $k \times (n-k)$ และจากสมการ $\mathbf{cH}^T = \mathbf{0}$ จะได้

$$[\mathbf{b} : \mathbf{m}][\mathbf{H}_1 : \mathbf{H}_2]^T = \mathbf{0} \tag{3.25}$$

แทนค่าเป็น

$$\mathbf{bH}_1 + \mathbf{mH}_2 = \mathbf{0} \tag{3.26}$$

จะได้

$$\mathbf{b} = \mathbf{mP} \tag{3.27}$$

โดย $\mathbf{P}$ ในที่นี้คือ เมทริกซ์สัมประสิทธิ์ (Coefficient matrix) หากข้อความอินพุทใดๆที่ไม่ใช่ศูนย์ทั้งหมดจะได้ความสัมพันธ์ของเมทริกซ์สัมประสิทธิ์ดังนี้

$$\mathbf{P}\mathbf{H}_1 + \mathbf{H}_2 = \mathbf{0} \tag{3.28}$$

และได้เมทริกซ์สัมประสิทธิ์ดังสมการด้านล่าง

$$\mathbf{P} = \mathbf{H}_2\mathbf{H}_1^{-1} \tag{3.29}$$

ดังนั้นเมทริกซ์กำเนิดได้สมการเป็น

$$\mathbf{G} = \left[\mathbf{P} : \mathbf{I}_k\right] = \left[\mathbf{H}_2\mathbf{H}_1^{-1} : \mathbf{I}_k\right] \tag{3.30}$$

โดยการเข้ารหัสของรหัสแอลดีพีซี มีสมการดังนี้

$$\mathbf{c} = \mathbf{m}\mathbf{G} \tag{3.31}$$

<u>ตัวอย่างที่ 3.9</u> วิธีการสร้างเมทริกซ์กำเนิดจากจากเมทริกซ์ตรวจสอบพาริตี้

กำหนดให้เมทริกซ์ตรวจสอบพาริตี้มีค่าเป็น

$$\mathbf{H} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 0 \end{bmatrix}$$

ทรานสโพสเมทริกซ์ตรวจสอบพาริตี้มีค่าเป็น

$$\mathbf{H}^T = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

เมื่อ $\mathbf{H} = [\mathbf{H}_1 : \mathbf{H}_2]$ จะได้

$$\mathbf{H}_1 = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix}, \quad \mathbf{H}_2 = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

ให้ $\mathbf{mH}_2 = \mathbf{u}$ จากสมการที่ (3.17) ดังนั้น

$$\begin{bmatrix} b_0 & b_1 & b_2 & b_3 & b_4 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \end{bmatrix} = \begin{bmatrix} u_0 & u_1 & u_2 & u_3 & u_4 \end{bmatrix}$$

จากสมการข้างบน ได้สมการการหลายตัวแปร ดังนี้

$$b_0 + b_1 + b_4 = u_0$$
$$b_0 + b_2 + b_3 = u_1$$
$$b_1 + b_3 + b_4 = u_2$$
$$b_0 + b_2 + b_4 = u_3$$
$$b_1 + b_2 + b_3 = u_4$$

ทำการแก้สมการ

$$b_0 = u_2 + u_3 + u_4$$
$$b_1 = u_1 + u_2 + u_3$$
$$b_2 = u_0 + u_1 + u_2$$
$$b_3 = u_0 + u_3 + u_4$$
$$b_4 = u_0 + u_1 + u_4$$

เมื่อ $\mathbf{b} = [\mathbf{u}]\mathbf{H}_1^{-1}$ สามารถเขียนให้อยู่ในรูปเมทริกซ์ดังนี้

$$\mathbf{b} = [\mathbf{u}]\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

ดังนั้น

$$\mathbf{H}_1^{-1} = \begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{H}_2\mathbf{H}_1^{-1} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}\begin{bmatrix} 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$$\mathbf{I}_k = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

หาค่าเมทริกซ์กำเนิดได้จาก $\mathbf{G} = [\mathbf{H}_2\mathbf{H}_1^{-1} : \mathbf{I}_k]$ ได้เมทริกซ์กำเนิดดังนี้

$$\mathbf{G} = \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

จากนั้นตรวจสอบความถูกต้องของเมทริกซ์กำเนิด โดยขั้นแรกทำการทดลองป้อนข้อความอินพุท $\mathbf{m}$ เพื่อทำการเข้ารหัสโดยเมทริกซ์กำเนิด สมมุติให้ $\mathbf{m} = [1 \quad 0 \quad 0 \quad 0 \quad 1]$ จะได้คำรหัสเป็น

$$\mathbf{c} = \mathbf{mG} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$

$$\mathbf{c} = [1 \quad 0 \quad 0 \quad 1 \quad 0 \quad 1 \quad 0 \quad 0 \quad 0 \quad 1]$$

จากคำรหัส $\mathbf{c}$ เป็นการเข้ารหัสเชิงระบบ คือมีบิตข้อความอินพุท $\mathbf{m}$ และบิตตรวจสอบ $\mathbf{b}$ ดังสมการที่ (3.22) จะได้คำรหัสเป็น $\mathbf{c} = [\mathbf{b} : \mathbf{m}]$ และการตรวจสอบความถูกต้องจากสมการ $\mathbf{cH}^T$

$$\mathbf{cH}^T = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 0 \end{bmatrix}$$

$$\mathbf{cH}^T = [0 \quad 0 \quad 0 \quad 0 \quad 0]$$

จาก $\mathbf{cH}^T$ มีค่าที่ได้เป็นเวกเตอร์ศูนย์ แสดงว่าเมทริกซ์กำเนิดที่คำนวณมีค่าถูกต้องสามารถนำไปใช้ในกระบวนการเข้ารหัสได้ จากกระบวนการเข้ารหัสเมื่อพิจารณาจากโครงสร้างของรหัสแอลดีพีซีแบบต่าง ๆ ที่ได้กล่าวถึงไปแล้วในหัวข้อก่อนหน้านี้ สามารถสรุปความซับซ้อนในการคูณระหว่างเมทริกซ์กำเนิดกับบิตข้อมูลอินพุท $O(.)$ และวิธีการเข้ารหัสเร็วได้ดังตารางที่ 3.3

ตารางที่ 3.3 ความซับซ้อนในการการเข้ารหัสและการเข้ารหัสแบบเร็วของโครงสร้างรหัสแอลดีพีซี

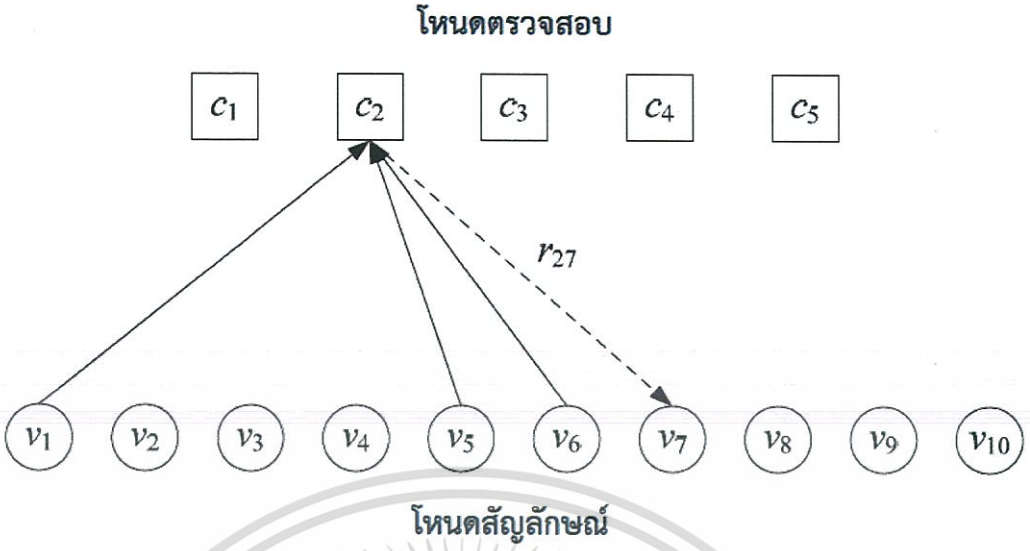
โครงสร้าง	ความซับซ้อน	การเข้ารหัสแบบเร็ว
รหัสอาเรย์, อัลกอริทึมพีอีจี	$O(n^2)$	ไม่มี
รหัสอาเรย์แบบปรับปรุง	$O(n)$	ใช้วิธีการของ Richardson [23] แต่ยังคงใช้วงจรคูณและวงจรบวกในวงจรเข้ารหัส
รหัสเรขาคณิตยูคลิด, เรขาคณิตเชิงภาพฉาย	$O((n-k)k)$	ใช้วงจรเรจิสเตอร์แบบเลื่อนที่มีการป้อนกลับ
รหัสควอไซไซคลิค, รหัสบล็อกไม่สมบูรณ์แบบสมดุล	$O((n-k)k)$	ใช้วงจร Cyclic shift register-adder-accumulator

ในส่วนของการถอดรหัสของรหัสแอลดีพีซี มีอยู่หลายแบบด้วยกัน ซึ่งประกอบไปด้วยอัลกอริทึมดังต่อไปนี้

3.6.1 อัลกอริทึมแบบรวมผลคูณ

เมทริกซ์ตรวจสอบพาริตี้สามารถแสดงให้อยู่ในรูปแบบของกราฟสองส่วน (Bipartite graph) หรือกราฟแทนเนอร์ (Tanner graph) โดยแต่ละแถวในเมทริกซ์ตรวจสอบพาริตี้แสดงให้เห็นถึงสมการตรวจสอบพาริตี้ กราฟแทนเนอร์ที่ใช้อธิบายความสัมพันธ์ของคำรหัสกับเมทริกซ์ตรวจสอบพาริตี้ สามารถนำมาประยุกต์ใช้ร่วมกับอัลกอริทึมแบบรวมผลคูณ (Sum-product algorithm) หรือกระบวนการส่งผ่านความเชื่อมั่น (Belief propagation algorithm) ไปบนเส้นทางระหว่างโหนดตรวจสอบและโหนดสัญลักษณ์กราฟแทนเนอร์ ดังรูปที่ 3.10 โดยโหนดตรวจสอบ C_2 จะมีความสัมพันธ์ดังนี้

$$v_1 + v_5 + v_6 + v_7 = 0 \tag{3.32}$$



รูปที่ 3.10 การส่งผ่านความเชื่อมั่นจากโหนดตรวจสอบไปยังโหนดสัญลักษณ์

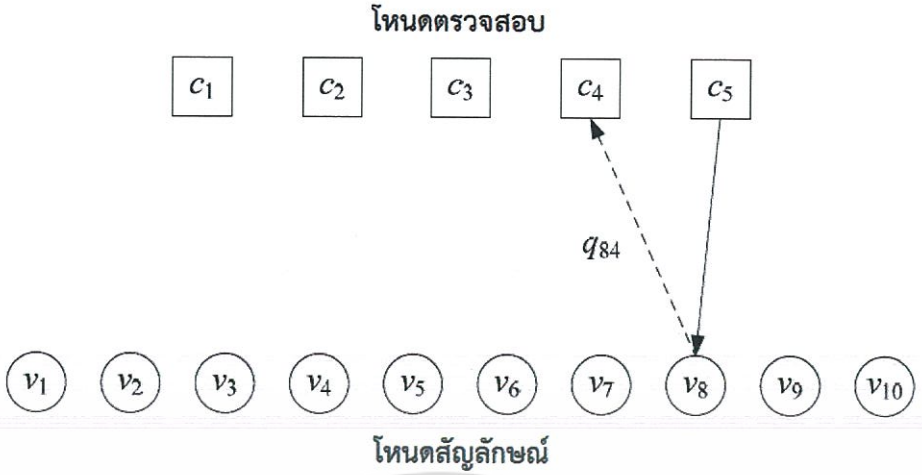
ข้อมูลที่ถูกส่งจากโหนดตรวจสอบ C_2 ไปยังโหนดสัญลักษณ์ v_7 ตามรูปที่ 5 และสามารถคำนวณหาได้จากข้อมูลที่ถูกส่งจากโหนดสัญลักษณ์ v_1, v_5 และ v_6 ไปยังโหนดตรวจสอบ C_2 ได้จาก

$$
\begin{aligned}
r_{27}(1) &= P(v_7 = 1, C_2 \mid y_i) \\
&= P(v_7 = 1, v_1 + v_5 + v_6 + v_7 = 0 \mid y_i) \\
&= P(v_1 + v_5 + v_6 = 1 \mid y_i) \\
&= p_{v1}(1-p_{v5})(1-p_{v6}) + p_{v5}(1-p_{v1})(1-p_{v6}) + \\
&\quad p_{v6}(1-p_{v1})(1-p_{v5}) + p_{v1}p_{v5}p_{v6} \\
&= \frac{1}{2} - \frac{1}{2}\prod_{i\in\{v1,v5,v6\}}(1-2p_i)
\end{aligned}
\tag{3.33}
$$

ความน่าจะเป็นที่ถูกส่งจากโหนดตรวจสอบไปยังโหนดสัญลักษณ์เขียนให้อยู่ในรูปทั่วไปได้ดังนี้

$$r_{ji}(0) = \frac{1}{2} - \frac{1}{2}\prod_{i\in C_j \setminus i}\left(1-2q_{ij}(1)\right) \tag{3.34}$$

$$r_{ji}(1) = 1 - r_{ji}(0) \tag{3.35}$$



รูปที่ 3.11 การส่งผ่านความเชื่อมั่นจากสัญลักษณ์ไปยังโหนดตรวจสอบ

ข้อมูลที่ถูกส่งจากโหนดสัญลักษณ์ v_8 ไปยังโหนดตรวจสอบ C_4 ตามรูปที่ 3.11 สามารถคำนวณหาได้จากข้อมูลที่ถูกส่งจากโหนดตรวจสอบ C_5 ไปยังโหนดสัญลักษณ์ v_8 ตามความสัมพันธ์ได้ดังนี้

$$q_{84}(0) = P(C_4 = 0, V_8 \mid y_i)$$

$$= K_{82}(1-P_8)\prod_{j\in\{c5\}} p_j \tag{3.36}$$

โดยที่ K_{82} คือค่าคงที่ทำให้ $q_{82}(0)+q_{82}(1)=1$ ซึ่งความน่าจะเป็นที่ถูกส่งจากโหนดสัญลักษณ์ไปยังโหนดตรวจสอบสามารถเขียนให้อยู่ในรูปทั่วไปได้ดังนี้

$$q_{ij}(0) = K_{ij}(1-P_i)\prod_{j\in V_i\setminus j} r_{j'i}(0) \tag{3.37}$$

$$q_{ij}(1) = K_{ij}P_i\prod_{j\in V_i\setminus j} r_{j'i}(1) \tag{3.38}$$

โดยที่ P_i คือความน่าจะเป็นที่สัญลักษณ์ i มีค่าเท่ากับ 1 ในกรณีของช่องสัญญาณรบกวนแบบสีขาว P_i หาได้จาก

$$P_i = \frac{1}{1+e^{-2y_i/\sigma^2}} \tag{3.39}$$

สรุปขั้นตอนถอดรหัสด้วยอัลกอริทึมแบบรวมผลคูณ

1. คำนวณค่าความน่าจะเป็น $q_{ij}(1)$ ที่ถูกส่งจากโหนดสัญลักษณ์ไปยังโหนดตรวจสอบ จากสัญญาณที่ได้รับ y_i โดยที่ i มีค่าเท่ากับ $1,2,...,n$ โดยหาได้จากสมการที่ (3.37) และความน่าจะเป็น $q_{ij}(0)$ จากสมการที่ (3.38)
2. คำนวณความน่าจะเป็น r_{ji} จากโหนดตรวจสอบทุกโหนด ไปยังโหนดสัญลักษณ์จากสมการที่ (3.34) และ (3.35)
3. ปรับปรุงค่า q_{ij} โดยใช้สมการที่ (3.37) และ (3.38) เพื่อใช้ในการวนรอบของการถอดรหัสถัดไป
4. คำนวณค่าซอฟต์เอาท์พุตในการถอดรหัสของแต่ละบิต i ตั้งแต่บิตที่ 1 ถึงบิตที่ n ผ่านสมการดังต่อไปนี้

$$Q_i(0) = K_i(1-P_i)\prod_{j\in V_i} r_{ji}(0) \tag{3.40}$$

$$Q_i(1) = K_i(P_i)\prod_{j\in V_i} r_{ji}(1) \tag{3.41}$$

โดยที่ K_i คือค่าคงซึ่งทำให้ $Q_i(0)+Q_i(1)=1$

5. ตัดสินใจสัญญาณที่ได้รับ y_i ด้วย

$$c_i = \begin{cases} 1, & L(Q_i) < 0 \\ 0, & L(Q_i) \le 0 \end{cases} \tag{3.42}$$

3.6.2 อัลกอริทึมแบบล็อกรวมผลคูณ

กระบวนการถอดรหัสแบบรวมผลคูณ ที่ผ่านมาไม่ได้รับความนิยมเท่าที่ควร เนื่องจากในกระบวนการจะประกอบไปด้วยโอเปอร์เรเตอร์การคูณเป็นจำนวนมาก ทำให้การสร้างอุปกรณ์ถอดรหัสทางฮาร์ดแวร์มีความซับซ้อนเพิ่มขึ้นตามรวมทั้งความเสถียรภาพของระบบลดลง จึงได้มีการประยุกต์ใช้ค่าล็อกการิทึมธรรมชาตินำมาช่วยปรับปรุงการถอดรหัส เรียกว่า อัลกอริทึมแบบล็อกรวมผลคูณ (Logarithmic sum-product algorithm) โดยจะนิยามอัตราส่วนความน่าจะเป็นแบบล็อก (Log Likelihood Ratios: LLRs) ดังต่อไปนี้

$$L(c_i) = \log\left(\frac{\Pr(c_i=0\,|\,y_i}{\Pr(c_i=0\,|\,y_i}\right) \tag{3.43}$$

$$L(r_{ji}) = \log\left(\frac{r_{ji}(0)}{r_{ji}(1)}\right) \tag{3.44}$$

$$L(q_{ij}) = \log\left(\frac{q_{ij}(0)}{q_{ij}(1)}\right) \tag{3.45}$$

$$L(Q_i) = \log\left(\frac{Q_i(0)}{Q_i(1)}\right) \tag{3.46}$$

ทั้งนี้ล็อกการิทึมมีฐานเป็น e และสมการที่ (3.34) ทำการแทน $r_{ji}(0)$ ด้วย $1-r_{ji}(1)$

$$1-2r_{ji}(1) = \prod_{i\in C_j\backslash i}\left(1-2q_{ij}(1)\right) \tag{3.47}$$

จากความสัมพันธ์ $\tanh\left(\frac{1}{2}\log\left(\frac{p_0}{p_1}\right)\right) = p_0 - p_1 = 1-2p_1$ ดังนั้น

$$\tanh\left(\frac{1}{2}L(r_{ji})\right) = \prod_{i\in C_j\backslash i}\tanh\left(\frac{1}{2}L(q_{ij})\right) \tag{3.48}$$

$$L(r_{ji}) = 2\tanh^{-1}\left(\prod_{i\in C_j\backslash i}\tanh\left(\frac{1}{2}L(q_{ij})\right)\right) \tag{3.49}$$

ให้ $L(q_{ij}) = \alpha_{ij}\beta_{ij}$ โดยที่ $\alpha_{ij} = sign[L(q_{ij})]$ และ $\beta_{ij} = |L(q_{ij})|$

$$L(r_{ji}) = \left(\prod_{i\in C_j\backslash i}\alpha_{ij}\right)2\tanh^{-1}\left(\prod_{i\in C_j\backslash i}\tanh\left(\frac{1}{2}\beta_{ij}\right)\right) \tag{3.50}$$

$$= \left(\prod_{i\in C_j\backslash i}\alpha_{ij}\right)2\tanh^{-1}\log^{-1}\log\left(\prod_{i\in C_j\backslash i}\tanh\left(\frac{1}{2}\beta_{ij}\right)\right) \tag{3.51}$$

$$= \left(\prod_{i\in C_j\backslash i}\alpha_{ij}\right)2\tanh^{-1}\log^{-1}\sum_{i\in C_j\backslash i}\log\left(\tanh\left(\frac{1}{2}\beta_{ij}\right)\right) \tag{3.52}$$

กำหนดให้ $\phi(x) = -\log[\tanh(x/2)] = \log(e^x+1)/(e^x-1)$ และ $\phi(x) = \phi^{-1}(x)$ ที่ $x>0$ ดังนั้น อัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโหนดตรวจสอบไปยังโหนดสัญลักษณ์คือ

$$L(r_{ji}) = \left(\prod_{i\in C_j\backslash i}\alpha_{ij}\right)\left(\phi\left(\sum_{i\in C_j\backslash i}\phi\left(\beta_{ij}\right)\right)\right) \tag{3.53}$$

อัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโหนดสัญลักษณ์ไปยังโหนดตรวจสอบหาได้โดยการนำสมการที่ (3.37) มาหารด้วย (3.38) ซึ่งจะได้ดังสมการที่ (3.54)

$$L(q_{ij}) = L(c_i) + \sum_{i \in V_i \setminus j} L(r_{ij}) \tag{3.54}$$

และทำการเปลี่ยนค่าซอฟต์เอาท์พุตของการถอดรหัสของแต่ละบิตให้อยู่ในรูป

$$L(Q_i) = L(c_i) + \sum_{i \in V_i} L(r_{ij}) \tag{3.55}$$

ตัดสินใจสัญญาณที่ได้รับด้วย

$$c_i = \begin{cases} 1, & L(Q_i) < 0 \\ 0, & L(Q_i) \leq 0 \end{cases} \tag{3.56}$$

สรุปขั้นตอนถอดรหัสด้วยอัลกอริทึมแบบล็อกรวมผลคูณ

1. คำนวณค่าความเชื่อมั่นที่ถูกส่งจากโหนดสัญลักษณ์ไปยังโหนดตรวจสอบจากสัญญาณที่ได้รับ y_i โดยที่ i มีค่าเท่ากับ $1, 2, ..., n$ โดยหาได้จากสมการที่ (3.43)
2. คำนวณค่าความเชื่อมั่น $L(r_{ji})$ ที่ถูกส่งจากโหนดตรวจสอบทุกโหนดไปยังโหนดสัญลักษณ์โดยใช้สมการที่ (3.53)
3. ปรับปรุงค่า $L(q_{ij})$ โดยใช้สมการที่ (3.54) เพื่อใช้ในการวนรอบของการถอดรหัสถัดไป
4. คำนวณค่าซอฟต์เอาท์พุตในการถอดรหัสของ ตั้งแต่บิตที่ 1 ถึงบิตที่ n ผ่านสมการที่ (3.55)
5. ตัดสินใจสัญญาณที่ได้รับ y_i ด้วยสมการที่ (3.56)

3.6.3 อัลกอริทึมแบบผลรวมต่ำสุด

กระบวนการถอดรหัสแบบผลรวมต่ำสุด (Min-sum algorithm) เป็นการลดความซับซ้อนลงจากอัลกอริทึมแบบล็อกรวมผลคูณ โดยใช้การประมาณค่าของอัตราส่วนความน่าจะเป็นแบบล็อกที่ถูกส่งจากโหนดตรวจ สอบไปยังโหนดสัญลักษณ์ ดังสมการ

$$L(r_{ji}) = \left(\prod_{i \in C_j \setminus i} \alpha_{ij} \right) \left(\phi \left(\sum_{i \in C_j \setminus i} \phi(\beta_{ij}) \right) \right) \approx \left(\prod_{i \in C_j \setminus i} \alpha_{ij} \right) \left(\phi \left(\phi \left(\min_{i \in C_j \setminus i} \beta_{ij} \right) \right) \right)$$

$$\approx \left(\prod_{i \in C_j \setminus i} \alpha_{ij} \right) \min_{i \in C_j \setminus i} \beta_{ij} \tag{3.57}$$

ในบทนี้ได้กล่าวถึงพื้นฐานของรหัสแอลดีพีซีและอธิบายโครงสร้างและวิธีการออกแบบเพื่อสร้างเมทริกซ์ตรวจสอบพาริตี้ในแบบต่าง ๆ หลายวิธี ซึ่งพอสรุปโครงสร้างต่าง ๆ ในการออกแบบได้ดังนี้ โครงสร้างรหัสอาเรย์ที่กำหนดเมทริกซ์เอกลักษณ์และหลักส่วนที่เหลือเป็นเมทริกซ์หมุนสลับตำแหน่ง โครงสร้างรหัสอาร์เรย์แบบปรับปรุงเป็นรหัสที่ปรับปรุงต่อมาจากรหัสอาเรย์เพื่อให้ได้สมรรถนะที่ดีขึ้นโดยรหัสแอลดีพีซีเป็นแบบไม่คงที่ โครงสร้างรหัสควอไซไซคลิคเป็นโครงสร้างที่นักวิจัยเสนอวิธีการออกแบบมากมายและมีวงจรรองรับในการเข้ารหัสเร็วซึ่งได้กล่าวไว้ในบทที่ 2 ในการนำไปสร้างฮาร์ดแวร์รวมทั้งมีความยืดหยุ่นสูงในการออกแบบอัตรารหัสค่าต่าง ๆ การออกแบบทำได้ด้วยการกำหนดเมทริกซ์หมุนสลับตำแหน่ง แต่ทั้งนี้วิธีการที่ออกแบบได้เกิรธมากกว่า 6 เป็นวิธีการที่น่าสนใจมากกว่าวิธีการได้เกิรธเท่ากับ 6 ในการพัฒนาเพื่อให้ได้สมรรถนะดียิ่งขึ้น แต่การออกแบบควรทำให้ง่ายขึ้นหรือครอบคลุมการสร้างเมทริกซ์ที่อัตรารหัสที่แตกต่างกัน โครงสร้างรหัสเรขาคณิตขอบเขตจำกัดเป็นรหัสที่ออกแบบบนพื้นฐานคณิตศาสตร์ขอบเขตจำกัดสามารถแบ่งออกเป็น 2 ประเภท คือ รหัสเรขาคณิตยูคลิดและรหัสเรขาคณิตเชิงภาพฉาย เป็นรหัสที่มีโครงสร้างเป็นรหัสไซคลิกและมีระยะห่างต่ำสุดที่สูงและมีวงจรที่ง่ายรองรับในการประยุกต์ใช้เป็นฮาร์ดแวร์แต่ทั้งนี้การนำไปใช้งานมีจำกัดในส่วนของอัตรารหัส กล่าวคือรหัสเรขาคณิตขอบเขตจำกัดสามารถออกแบบสำหรับอัตรารหัสต่าง ๆ ได้ไม่มาก โครงสร้างรหัสบีไอบีดีเป็นโครงสร้างที่ออกแบบจากพื้นฐานคณิตศาสตร์ขอบเขตจำกัดที่กำหนดน้ำหนัก 1 ในแนวตั้งมีค่าเท่ากับ 4 และ 5 และมีเกิรธเท่ากับ 6 และโครงสร้างอัลกอริทึมพีอีจีเป็นโครงสร้างแบบสุ่มเพื่อสร้างให้ได้เกิรธที่มีขนาดใหญ่มีสมรรถนะที่ดีมากแต่ไม่เหมาะสำหรับการประยุกต์ใช้งานจริงเนื่องจากเป็นโครงสร้างแบบสุ่ม จากโครงสร้างทั้งหมดที่ได้กล่าวไว้ในบทนี้ ผู้วิจัยเลือกโครงสร้างรหัสควอไซไซคลิคเพื่อออกแบบให้ได้เกิรธที่ใหญ่และต้องเป็นวิธีการออกแบบง่ายไม่ซับซ้อนรวมทั้งสามารถที่ออกแบบรองรับกับอัตรารหัสค่าต่าง ๆ ได้ซึ่งจะได้นำเสนอในบทถัดไป

บทที่ 4
วิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้และผลการทดลอง

บทนี้แสดงวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ของงานวิจัยนี้ โดยนำเสนอวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้โดยออกแบบบนพื้นฐานของรหัสควอไซไซคลิคโดยใช้เมทริกซ์หมุนสลับตำแหน่ง ในการออกแบบวิธีแรกจะนำเสนอวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ปราศจากลูป 4 และวิธีการที่สองจะนำเสนอวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ปราศจากลูป 6 เพื่อสร้างเกิรธที่มีขนาดใหญ่กว่าหรือเท่ากับ 8 จากการนำเสนอวิธีการออกแบบทั้งสองวิธีแล้วจะทำการเปรียบเทียบประสิทธิภาพของวิธีการทั้งสองแบบและเปรียบเทียบกับวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ใช้วิธีการออกแบบที่ใช้วิธีออกแบบในประเภทเดียวกันหรือคล้ายคลึงกัน เช่น รหัสอาเรย์, รหัสอาเรย์แบบปรับปรุง และรหัสควอไซไซคลิคในรูปแบบต่าง ๆ นอกจากนั้นวิธีการออกแบบที่ได้นำเสนอจะทำการเปรียบเทียบกับรูปแบบการออกแบบเมทริกซ์ตรวจสอบพาริตี้สำหรับรหัสแอลดีพีซีในแบบต่าง ๆ ที่ไม่ใช่วิธีออกแบบในประเภทเดียวกันซึ่งที่ได้กล่าวแล้วในบทที่ 3 เพื่อแสดงให้เห็นถึงเปรียบเทียบประสิทธิภาพวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ของงานวิจัยนี้ว่ามีประสิทธิดีเพียงใด โดยในการทดสอบจะทำการทดลองบนช่องสัญญาณเกาส์เซียนและเปรียบเทียบค่าผิดพลาด เช่น อัตราบิตผิดพลาด (Bit Error Rate: BER), อัตราเฟรมผิดพลาด (Frame Error Rate: FER) ต่ออัตราสัญญาณรบกวน E_b / N_0 (SNR)

4.1 การออกแบบรหัสควอไซไซคลิคแอลดีพีซีโดยปราศจากลูป 4

วิธีการออกแบบรหัสแอลดีพีซีด้วยวิธีการนี้ [24][25][26] จะกำหนดขนาดเมทริกซ์หมุนสลับตำแหน่งเป็นเมทริกซ์ที่มีการเลื่อนข้อมูลไปทางขวาจากเมทริกซ์เอกลักษณ์มีขนาดเป็นจำนวนเลขเฉพาะ (Prime Number) เพื่อให้ไม่เกิดลูป 4 ภายในเมทริกซ์ตรวจสอบพาริตี้ ดังสมการที่ (3.1) และโครงสร้างในการออกแบบเมทริกซ์ตรวจสอบพาริตี้มีโครงสร้างเช่นเดียวกันกับสมการที่ (3.3) โดยกำหนดให้ 1 ในที่นี้คือ เมทริกซ์หมุนสลับตำแหน่งที่เลื่อนไปทางขวาจากเมทริกซ์เอกลักษณ์ 1 ครั้ง, a คือ เมทริกซ์หมุนสลับตำแหน่งที่เลื่อนไปทางขวาจากเมทริกซ์เอกลักษณ์ a ครั้ง, b คือ เมทริกซ์หมุนสลับตำแหน่งที่เลื่อนไปทางซ้ายจากเมทริกซ์เอกลักษณ์ b ครั้ง, j คือน้ำหนัก 1 ในแนวตั้งภายในเมทริกซ์พาริตี้เชค $\mathbf{H}$, k คือน้ำหนัก 1 ในแนวตั้งภายในเมทริกซ์พาริตี้เชค $\mathbf{H}$ และ p คือขนาดของเมทริกซ์หมุนสลับตำแหน่งที่มีขนาดเป็นเลขจำนวนเฉพาะ ในการออกแบบทำได้โดยการหากำหนดค่าอิลิเมนต์ a และ b โดยที่ค่าอิลิเมนต์ต้องมีค่ามากกว่า 1 และน้อยกว่าขนาดของเมทริกซ์หมุนสลับตำแหน่ง p หรือ $1 < a, b < p$

การเลือกค่าอิลิเมนต์ในงานวิจัยนี้ขั้นตอนแรกในการออกแบบใช้คณิตศาสตร์ที่เรียกว่าลำดับเรขาคณิต (Geometric sequence) โดยคณิตศาสตร์นี้คือ ลำดับตัวเลข โดยแต่ละเทอมทำการคูณ

กัน ลำดับของจำนวนซึ่งอัตราส่วนของสมาชิกสองตัวที่อยู่ติดกันในลำดับเป็นค่าคงตัวที่ไม่เป็นศูนย์ โดยลักษณะสำคัญของลำดับเรขาคณิตคือพจน์ถัดไปจะเพิ่มขึ้นหรือลดลงทีละเท่าตัว ดังสมการที่ (4.1)

$$a_n = a_1 r^{n-1} \tag{4.1}$$

เมื่อ a_n คือ พจน์ที่ n ของลำดับเรขาคณิต, a_1 คือ พจน์แรกของลำดับเรขาคณิต, r คือ อัตราส่วนร่วม และ n คือ สมาชิกลำดับที่ n ของลำดับเรขาคณิต โดยวิธีการคำนวณหาลำดับสมาชิกดังตัวอย่างที่ 4.1

ตัวอย่างที่ 4.1 ให้ $a_1 = 1, r = 2$ และ $n = 10$ จากสมการที่ (4.1) จะได้

$$a = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\}$$

จากลำดับเรขาคณิตหากนำมาใช้ในสนามขอบเขตจำกัด ค่าที่ได้ต้องทำการมอดูโลด้วยค่าในฟิลด์ที่จำกัดไว้ ซึ่งในการออกแบบรหัสแอลดีพีซีก็คือค่าของขนาดเมทริกซ์หมุนสลับตำแหน่ง จากตัวอย่างที่ 4.1 หากกำหนดให้ขนาดของเมทริกซ์หมุนสลับตำแหน่งมีค่าเท่ากับ 31 ดังนั้นค่าที่ได้จากตัวอย่างที่ 4.1 ต้องกระทำใน $GF(31)$ จะได้

$$a_{GF(31)} = \{1, 2, 4, 8, 16, 32, 64, 128, 256, 512\} \bmod 31$$

$a_{GF(31)} = \{1, 2, 4, 8, 16, 1, 2, 4, 8, 16\}$ ค่าที่ได้จะมีค่าอยู่ในช่วง 0 ถึง 30 เท่านั้น

ในการออกแบบเมทริกซ์ตรวจสอบพาริตี้ในงานวิจัยนี้กำหนดให้เมทริกซ์หมุนสลับตำแหน่งในแต่ละแถวต้องมีค่าในการหมุนของเมทริกซ์หมุนสลับตำแหน่งไม่ซ้ำกัน ดังนั้นค่าที่ได้ $a_{GF(31)}$ จะมีเหลือสมาชิกเพียง 5 ค่า ดังนั้น $a_{GF(31)} = \{1, 2, 4, 8, 16\}$

จากตัวอย่างที่ 4.1 เป็นวิธีการหาสมาชิกของค่าอิลิเมนต์ว่าขนาดของสมาชิกมีจำนวนเท่าใดเพื่อใช้ในการกำหนดค่าอิลิเมนต์ในการสร้างเมทริกซ์ตรวจสอบพาริตี้ ในการออกแบบด้วยวิธีนี้สำหรับอัตรารหัสที่ต่ำสามารถเลือกกำหนดอิลิเมนต์ใดๆสำหรับอิลิเมนต์ a และ b สร้างเมทริกซ์พาริตี้เชคได้ค่อนข้างกว้าง แต่สำหรับอัตราที่สูงขึ้นหรืออัตรารหัสที่สูงมากจำเป็นที่จะต้องหาค่าอิลิเมนต์ที่เหมาะสมเพื่อค่าที่อิลิเมนต์ที่กำหนดต้องไม่เกิดการซ้ำค่าของแต่ละแถวของค่าเมทริกซ์หมุนสลับตำแหน่ง เพราะจะทำให้เกิดลูป 4 ขึ้นในระบบ การหาค่าที่เหมาะสมทำได้โดยการใส่ค่าอิลิเมนต์ทุกค่าตั้งแต่ 2 ถึง p -1 ลงไปและหาว่าค่าอิลิเมนต์ใดได้สมาชิกครบทุกค่า พิจารณาดังตัวอย่างต่อไปนี้

<u>ตัวอย่างที่ 4.2</u> การออกแบบรหัสควอไซไซคลิคแอลดีพีซี อัตรารหัส 0.9, น้ำหนัก 1 ในแนวตั้ง j เท่ากับ 3, น้ำหนัก 1 ในแนวนอน k เท่ากับ 3 และขนาดเมทริกซ์หมุนสลับตำแหน่ง p เท่ากับ 31 วิธีการเลือกค่าอิลิเมนต์ทำได้จากการนำค่าอิลิเมนต์ตั้งแต่ 2 ถึง p -1 เพื่อหาค่าที่ได้เซตที่มีสมาชิกครบทุกค่า เช่น อิลิเมนต์ค่าเท่ากับ 2 จะทำการยกกำลัง n โดย n มีค่าตั้งแต่ $0 \le n \le p-1$ และค่าที่ได้จากการยกกำลังให้ทำการมอดูโลด้วยค่า p ที่มีเท่ากับ 31 จะได้ค่าเซตของอิลิเมนต์ต่าง ๆ เช่น อิลิเมนต์ 2 ได้เซต $S_2 = \{1,2,4,8,16\}$ ทำการหาค่าสมาชิกของเซตในทุกอิลิเมนต์จะได้ค่าดังนี้

$S_2 = \{1,2,4,8,16\}$,

$S_3 = \{1,3,9,27,19,26,16,17,20,29,25,13,8,24,10,30,28,22,4,12,5,15,14,11,2,6,18,23,7,21\}$,

$S_4 = \{1,4,16,2,8\}$,

$S_5 = \{1,5,25\}$,

$S_6 = \{1,6,5,30,25,26\}$,

$S_7 = \{1,7,18,2,14,5,4,28,10,8,25,20,16,19,9\}$,

$S_8 = \{1,8,2,16,4\}$,

$S_9 = \{1,9,19,16,20,25,8,10,28,4,5,14,2,18,7\}$,

$S_{10} = \{1,10,7,8,18,25,2,20,14,16,5,19,4,9,28\}$,

$S_{11} = \{1,11,28,29,9,6,4,13,19,23,5,24,16,21,14,30,20,3,2,22,25,27,20,14,16,5,19,4,9,28\}$,

$S_{12} = \{1,12,20,23,28,26,2,24,9,15,25,21,4,17,18,30,19,11,8,3,5,29,7,22,16,6,10,27,14,13\}$,

$S_{13} = \{1,13,14,27,10,6,16,22,7,29,5,3,8,11,19,30,18,17,4,21,25,15,9,24,2,26,28,23,20,12\}$,

$S_{14} = \{1,14,10,16,7,5,8,19,18,4,25,9,2,28,20\}$,

$S_{15} = \{1,15,8,27,2,30,16,23,4,29\}$,

$S_{16} = \{1,16,8,4,2\}$,

$S_{17} = \{1,17,10,15,7,26,8,12,18,27,25,22,2,3,20,30,14,21,16,24,5,23,19,13,4,6,9,29,28,11\}$,

$S_{18} = \{1,18,14,4,10,25,16,9,7,2,5,28,8,20,19\}$,

$S_{19} = \{1,19,20,8,28,5,2,7,9,16,25,10,4,14,18\}$,

$S_{20} = \{1,20,28,2,9,25,4,18,19,8,5,7,16,10,14\}$,

$S_{21} = \{1,21,7,23,18,6,2,11,14,15,5,12,4,22,28,30,10,24,8,13,25,29,20,17,16,26,19,27,9,3\}$,

$S_{22} = \{1,22,19,15,20,6,8,21,28,27,5,17,2,13,7,30,9,12,16,11,25,23,10,3,4,26,14,29,18,24\}$,

$S_{23} = \{1,23,2,15,4,30,8,29,16,27\}$,

$S_{24} = \{1,24,18,29,14,26,4,3,10,23,25,11,16,12,9,30,7,13,2,17,5,27,28,21,8,6,20,15,19,22\}$,

$S_{25} = \{1,25,5\}$,

$S_{26} = \{1,26,25,30,5,6\}$,

$S_{27} = \{1,27,16,29,8,30,4,15,2,23\}$,

$S_{28} = \{1,28,9,4,19,5,16,14,20,2,25,18,8,7,10\}$,

$S_{29} = \{1,29,4,23,16,30,2,27,8,15\}$,

$S_{30} = \{1,30\}$

จากการคำนวณจากกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p เซตที่มีสมาชิกครบทุกค่า คือ $S_3, S_{11}, S_{12}, S_{13}, S_{17}, S_{21}, S_{22}, S_{24}$ และเซตที่มีอิลิเมนต์เป็นเลขจำนวนเฉพาะของกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p คือ $S_3, S_{11}, S_{13}, S_{17}$ ในที่นี้เลือกอิลิเมนต์เท่ากับ 3 แทนค่าเมทริกซ์หมุนสลับตำแหน่งลงในแถวแรก หรือ แทนค่าอิลิเมนต์ a เท่ากับ 3

$$\begin{bmatrix} 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 \\ - & - \\ - & - \end{bmatrix}$$

จากการคำนวณกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p เซตร่วมที่มีสมาชิกเท่ากับ 3 ค่า คือ S_5, S_{25} และเซตที่อิลิเมนต์เป็นเลขจำนวนเฉพาะของกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p คือ S_5 ดังนั้นจึงแทนค่าอิลิเมนต์ b เท่ากับ 5

$$\begin{bmatrix} 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 \\ 5 & - \\ 25 & - \end{bmatrix}$$

จากการคำนวณเมื่อได้เมทริกซ์หมุนสลับตำแหน่งแถวแรกและหลักแรกของเมทริกซ์พาริตี้เชคแล้ว ทำการคำนวณหาค่าสำหรับเมทริกซ์หมุนสลับตำแหน่งในตำแหน่งอื่นๆ โดยนำมาเมทริกซ์หมุนสลับตำแหน่งในแถวแรกมาคูณกับค่าอิลิเมนต์ในหลักแรกและมอดูโลด้วยขนาดของเมทริกซ์หมุนสลับตำแหน่ง p ดังนี้

$5\times[1\ 3\ 9\ 27\ 19\ 26\ 16\ 17\ 20\ 29\ 25\ 13\ 8\ 24\ 10\ 30\ 28\ 22\ 4\ 12\ 5\ 15\ 14\ 11\ 2\ 6\ 18\ 23\ 7\ 21]$

$25\times[1\ 3\ 9\ 27\ 19\ 26\ 16\ 17\ 20\ 29\ 25\ 13\ 8\ 24\ 10\ 30\ 28\ 22\ 4\ 12\ 5\ 15\ 14\ 11\ 2\ 6\ 18\ 23\ 7\ 21]$

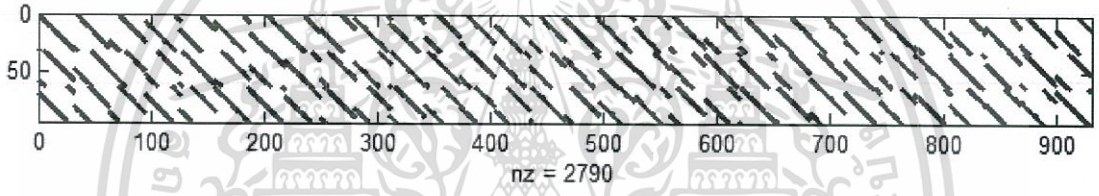
โดยการคูณหากค่าที่ได้มากกว่า p ต้องทำการมอดูโลด้วย p เมื่อคำนวณหาค่าเมทริกซ์หมุนสลับตำแหน่งทุกตำแหน่งจะได้เมทริกซ์พาริตี้เชคดังนี้

$$\begin{bmatrix} 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 \\ 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 & 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 \\ 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 & 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 \end{bmatrix}$$

หากพิจารณาเมทริกซ์ตรวจสอบพาริตี้ที่ได้ เห็นได้ว่าเมทริกซ์ย่อยในแถวที่ 2 และ 3 มีค่าเหมือนกับเมทริกซ์ย่อยในแถวที่ 1 เพียงแต่มีการเลื่อนตำแหน่งออกไป

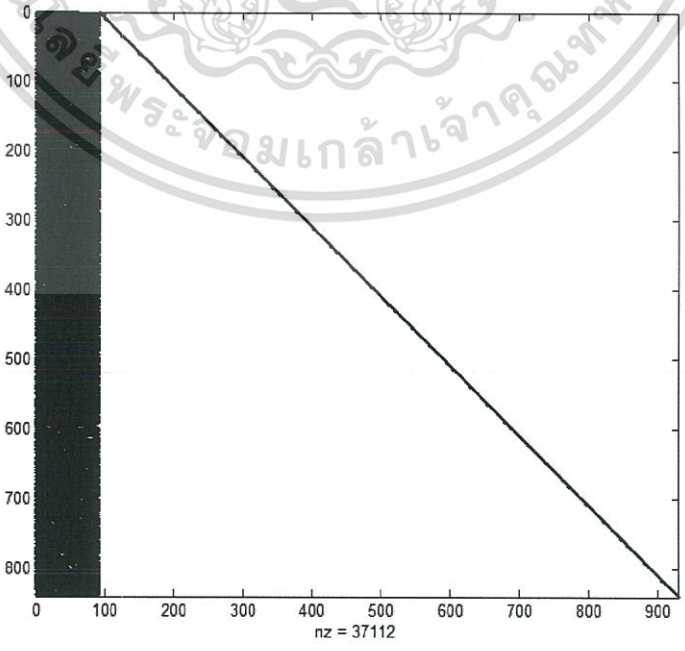
$$\left[\begin{array}{ccccccccc|ccccccccccc|ccccccccc} 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 \\ 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 & 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 \\ 25 & 13 & 8 & 24 & 10 & 30 & 28 & 22 & 4 & 12 & 5 & 15 & 14 & 11 & 2 & 6 & 18 & 23 & 7 & 21 & 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 \end{array}\right]$$

เช่นเดียวกัน หากแบ่งเมทริกซ์ตรวจสอบพาริตี้ออกเป็น 3 ส่วน เห็นได้ว่าในหลักที่ 1 ถึงหลักที่ 10 มีรูปแบบเหมือนกันกับหลักที่ 11 ถึง 20 และหลักที่ 21 ถึงหลักที่ 30 แต่จะต่างตรงที่มีการหมุนตำแหน่งขึ้นลงในแต่ละช่วง



รูปที่ 4.1 เมทริกซ์ตรวจสอบพาริตี้ที่ได้จากการออกแบบในตัวอย่างที่ 4.1

จากเมทริกซ์พาริตี้ตรวจสอบพาริตี้เมื่อทำการหาเมทริกซ์กำเนิดจะได้ดังรูปที่ 4.2



รูปที่ 4.2 เมทริกซ์กำเนิดสำหรับเมทริกซ์ตรวจสอบพาริตี้ที่ได้จากการออกแบบในตัวอย่างที่ 4.1

เมื่อได้เมทริกซ์กำเนิด $\mathbf{G}$ จะสามารถคำนวณหาค่าอัตรารหัสที่ใช้งานจริงโดยหาได้จากขนาดของเมทริกซ์กำเนิด 839×930 ดังนั้นอัตรารหัสที่ใช้งานจริงเท่ากับ 839/930=0.9002 โดยจะเป็นจำนวนบิตข้อมูลข่าวสาร 839 บิตและเป็นบิตตรวจสอบ 930-839=91 บิต เห็นได้ว่าอัตรารหัสในการออกแบบจะไม่เท่ากับอัตราในการใช้งานจริง ดังนั้นในการออกแบบรหัสแอลดีพีซีด้วยโครงสร้างนี้จะได้อัตรารหัสจริงจากการคำนวณจากเมทริกซ์กำเนิดเท่านั้น

นอกจากการกำหนดค่าเพื่อเลือกอิลิเมนต์ a และ b หากกำหนดให้อิลิเมนต์ $a=b$ จากสมการที่ (3.3) จะได้รูปแบบของเมทริกซ์ตรวจสอบพาริตี้ใหม่ขึ้นมาซึ่งรูปแบบของเมทริกซ์ได้ดังสมการที่ (4.2)

$$\mathbf{H}=\begin{bmatrix} 1 & a & a^2 & \cdots & a^{k-1} \\ a & a^2 & a^3 & \cdots & a^{k} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a^{k-1} & a^{k} & a^{k+1} & \cdots & a^{2(k-1)} \end{bmatrix}_{kp\times kp} \tag{4.2}$$

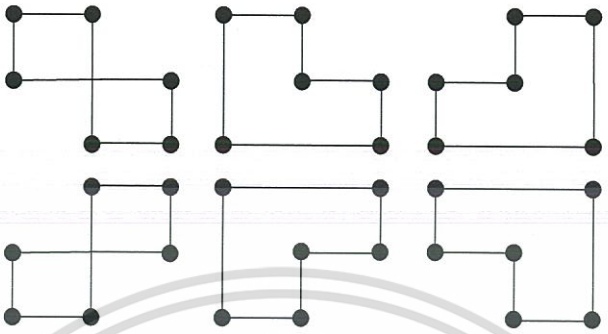
จากสมการที่ (4.2) ในการออกแบบจะทำได้โดยง่ายเนื่องจากการกำหนดเพื่อเลือกอิลิเมนต์ทำได้โดยการเลือกอิลิเมนต์ a เพียงค่าเดียว และหากเลือกค่าอิลิเมนต์เป็นค่าที่มีเซตที่มีสมาชิกครบทุกค่าแล้วเมทริกซ์ตรวจสอบพาริตี้ที่ได้จะเป็นแบบเมทริกซ์เต็มจำนวน การออกแบบนี้จะคำนวณเพียงแค่ค่าเมทริกซ์ย่อยของเมทริกซ์ตรวจสอบพาริตี้เพียงแถวแรกเพียงแถวเดียวเท่านั้น เพราะแถวที่สองก็คือการเลื่อนข้อมูลเมทริกซ์ย่อยจากแถวแรกไปทางซ้าย 1 ครั้ง ส่วนแถวถัดๆไปก็เลื่อนข้อมูลจากเมทริกซ์ในแถวก่อนหน้าทีละครั้งจนครบตามน้ำหนัก 1 ในแนวตั้งที่ต้องการ

วิธีการที่นำเสนอที่ได้จากสมการที่ (4.2) เป็นแนวทางในการเลือกอิลิเมนต์เพื่อสร้างเมทริกซ์ตรวจสอบพาริตี้โดยมีเงื่อนไขคือ ขนาดของเมทริกซ์หมุนสลับตำแหน่งต้องเป็นเลขจำนวนเฉพาะ การเลือกอิลิเมนต์ใดๆเมื่อสร้างเป็นเมทริกซ์ตรวจสอบพาริตี้จะต้องไม่มีค่าซ้ำในแต่ละแถวและหลักของเมทริกซ์ย่อย การออกแบบสำหรับอัตรารหัสสูงควรเลือกอิลิเมนต์ที่มีสมาชิกครบทุกค่า แต่ทั้งนี้วิธีการที่นำเสนอทั้ง 2 วิธีได้เกิรธเท่ากับ 6 เท่านั้น การออกแบบเพื่อเพิ่มประสิทธิภาพด้วยวิธีการที่ได้นำเสนอนี้สามารถที่จะปรับปรุงด้วยการเพิ่มเติมวิธีการเพื่อสร้างให้เมทริกซ์ตรวจสอบพาริตี้มีเกิรธตั้งแต่ 8 ขึ้นไปซึ่งจะนำเสนอในหัวข้อถัดไป

4.2 การออกแบบรหัสควอไซไซคลิคแอลดีพีซีเพื่อให้ได้เกิรธเท่ากับ 8

จากแนวคิดของ Jen-Fa Huang [16] ที่ออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ใช้เลือกลำดับที่เหมาะสมจากโครงสร้างเมทริกซ์ของตรวจสอบพาริตี้ที่ออกเสนอโดย Tanner [13] และสร้างเมทริกซ์ที่มีขนาดของเกิรธมากกว่า 6 ซึ่งแสดงให้เห็นว่าเมทริกซ์จากสมการที่ (3.3) ในบทที่ 3 สามารถที่จะกำหนดเลือกตำแหน่งในหลักและแถวที่เหมาะสมเพื่อสร้างเมทริกซ์ที่มีเกิรธขนาดใหญ่ได้ และจากหัวข้อก่อนหน้านี้ได้นำเสนอวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ไปราศจากเกิรธ 4 ในหัวข้อนี้จะ

ได้นำเสนอการปรับปรุงวิธีการออกแบบจากหัวข้อที่แล้ว โดยแนวคิดในการออกแบบเมทริกซ์พาริตี้โดยปราศจากลูป 6 มาจากวิธีการพิจารณาไซเคิล 6 ของเมทริกซ์พาริตี้ที่ได้ออกแบบด้วยวิธีการที่ได้นำเสนอในการสร้างเมทริกซ์ที่ปราศจากลูป 4 ในหัวข้อแรกจากสมการที่ (4.1)



รูปที่ 4.3 รูปแบบทั้งหมดของไซเคิล 6 ในเมทริกซ์ตรวจสอบพาริตี้

จากรูปที่ 4.3 รูปแบบของไซเคิล 6 มีอยู่ทั้งหมดอยู่ 6 รูปแบบ ดังนั้นในการที่จะสร้างเมทริกซ์ตรวจสอบพาริตี้ต้องไม่มีรูปแบบของไซเคิล 6 อยู่ในเมทริกซ์ที่จะทำการออกแบบ เมื่อพิจารณาสมการที่ (4.2) หากทำการออกแบบรหัสแบบเมทริกซ์เต็มจำนวน (Full Rank) จะมีเกิรธค่าเท่ากับ 6 แต่หากต้องการออกแบบรหัสแอลดีพีซีที่อัตรารหัสที่ต่ำลงมาจะเลือกเพียงบางแถวหรือบางหลักเท่านั้น ในการกำหนด น้ำหนัก 1 ในแนวตั้งเพื่อออกแบบให้ได้เกิรธขนาดใหญ่จะกำหนดให้มีค่าเท่ากับ 3 เนื่องจากหากกำหนดค่าดังกล่าวมีค่ามากกว่า 3 จะทำให้เกิดการเชื่อมต่อกันระหว่างโหนดและทำให้การสร้างเกิรธขนาดใหญ่เป็นไปได้ยากหรือเป็นไปไม่ได้ ส่วนการกำหนดค่าที่ต่ำกว่า 3 หรือกำหนดค่าน้ำหนัก 1 ในแนวตั้งเท่ากับ 2 จะง่ายต่อการสร้างเกิรธขนาดใหญ่แต่จะส่งผลต่อระยะห่างต่ำสุด กล่าวคือระยะห่างต่ำสุดที่ได้จะมีค่าต่ำโดยพิจารณาจากสมการที่ (3.5) และส่งผลต่อประสิทธิภาพและ Error floor ดังนั้นในงานวิจัยนี้จะกำหนด น้ำหนัก 1 ในแนวตั้งในการออกแบบเท่ากับ 3 หากพิจารณาเมทริกซ์ตรวจสอบพาริตี้จากสมการที่ (4.2) ถ้ากำหนดให้ขนาดของเมทริกซ์ประกอบด้วยเมทริกซ์ย่อยขนาด 3×3 โดยเลือกหลักที่ 1 ถึงหลักที่ 3 ดังสมการที่ (4.3)

$$\mathbf{H}=\begin{bmatrix} 1 & a & a^2 \\ a & a^2 & a^3 \\ a^2 & a^3 & a^4 \end{bmatrix}_{kp\times kp} \tag{4.3}$$

จากสมการที่ (4.3) พบว่าเมทริกซ์มีรูปแบบของเกิรธ 6 อยู่ 2 รูปแบบ คือ

$$\mathbf{H}=\begin{bmatrix} - & a & a^2 \\ a & a^2 & - \\ a^2 & - & a^4 \end{bmatrix}_{kp\times kp}, \mathbf{H}=\begin{bmatrix} 1 & - & a^2 \\ - & a^2 & a^3 \\ a^2 & a^3 & - \end{bmatrix}_{kp\times kp} \quad (4.4)$$

จากสมการที่ (4.4) สังเกตุรูปแบบของเกิรธ 6 นั้นเกิดจากค่า a^2 มีอยู่ 3 ตัวและมีอยู่ทุกแถวทุกหลัก จากสมการที่ (4.3) หากทดลองเลือกเมทริกซ์ย่อยขนาด 3×3 ใหม่อีกครั้งโดยเลือกตัดหลักใดหลักหนึ่งในหลักที่ 1 ถึงหลักที่ 3 และต่อด้วยหลักที่ 4 จะได้เมทริกซ์ดังนี้

$$\mathbf{H}_{2,3,4}=\begin{bmatrix} a & a^2 & a^3 \\ a^2 & a^3 & a^4 \\ a^3 & a^4 & a^5 \end{bmatrix}_{kp\times kp}, \mathbf{H}_{1,2,4}=\begin{bmatrix} 1 & a & a^3 \\ a & a^2 & a^4 \\ a^2 & a^3 & a^5 \end{bmatrix}_{kp\times kp}, \mathbf{H}_{1,3,4}=\begin{bmatrix} 1 & a^2 & a^3 \\ a & a^3 & a^4 \\ a^2 & a^4 & a^5 \end{bmatrix}_{kp\times kp} \quad (4.4)$$

จากสมการที่ (4.4) เมื่อนับจำนวนเกิรธของ $\mathbf{H}_{2,3,4}$ ยังคงมีเกิรธ 6 อยู่ทั้งนี้เนื่องมีค่า a^3 อยู่ 3 ตัว ส่วนเมทริกซ์ $\mathbf{H}_{1,2,4}$ และ $\mathbf{H}_{1,3,4}$ นั้นปราศจากเกิรธ 6

จากแนวคิดดังกล่าวจึงพอสรุปได้ว่าการสร้างเมทริกซ์ตรวจสอบพาริตี้ที่ต้องการเกิรธมากกว่า 6 คือ

1. กำหนดค่าขนาดของเมทริกซ์หมุนสลับตำแหน่ง p ต้องเป็นเลขจำนวนเฉพาะ
2. เลือกค่าอิลิเมนต์ที่ในเซตมีสมาชิกครบทุกค่า $a=\{1,2,...,p-1\}$ จากสมการที่ (4.1)
3. สร้างเมทริกซ์ตรวจสอบพาริตี้แบบเต็มจำนวน (Full rank) จากอิลิเมนต์ a จากสมการที่ (4.2)
4. ในกรณีที่ต้องการออกแบบที่อัตรารหัสต่ำลงมาจากเมทริกซ์ตรวจสอบพาริตี้แบบเต็มจำนวนให้เลือกหลักบางหลัก โดยมีเงื่อนไขว่าต้องไม่มีค่าเมทริกซ์หมุนสลับตำแหน่งซ้ำกันเกิน 2 ค่า
5. นำหลักมาต่อกันจนได้อัตรารหัสที่ต้องการและนับจำนวนเกิรธของเมทริกซ์ตรวจสอบพาริตี้เพื่อตรวจสอบว่าเมทริกซ์ที่ได้มีเกิรธเท่ากับ 8

<u>ตัวอย่างที่ 4.3</u> การออกแบบรหัสควอไซไซคลิคแอลดีพีซี อัตรารหัส 0.5, น้ำหนัก 1 ในแนวตั้ง j เท่ากับ 3, น้ำหนัก 1 ในแนวนอน k เท่ากับ 6 และขนาดเมทริกซ์หมุนสลับตำแหน่ง p เท่ากับ 101 ได้อิลิเมนต์เท่ากับ 2 ที่สามารถสร้างเมทริกซ์เต็มจำนวน (Full Rank) ขนาด $3p\times100p$

$$\mathbf{H}_{\text{full rank}}=\begin{bmatrix} 1 & 2 & 4 & 8 & 16 & 32 & 64 & 27 & 54 & \cdots & \cdots & \cdots & 38 & 76 & 51 \\ 2 & 4 & 8 & 16 & 32 & 64 & 27 & 54 & 7 & \cdots & \cdots & \cdots & 76 & 51 & 1 \\ 4 & 8 & 16 & 32 & 64 & 27 & 54 & 7 & 14 & \cdots & \cdots & \cdots & 51 & 1 & 2 \end{bmatrix}_{3p\times100p}$$

ทำการแบ่งเป็นเมทริกซ์ย่อยเป็นขนาด 3×3

$$\mathbf{H}_{\text{full rank}} = \left[\begin{array}{ccc|ccc|ccc|c|ccc} 1 & 2 & 4 & 8 & 16 & 32 & 64 & 27 & 54 & \cdots & 38 & 76 & 51 \\ 2 & 4 & 8 & 16 & 32 & 64 & 27 & 54 & 7 & \cdots & 76 & 51 & 1 \\ 4 & 8 & 16 & 32 & 64 & 27 & 54 & 7 & 14 & \cdots & 51 & 1 & 2 \end{array}\right]$$

จากเมทริกซ์ย่อยเป็นขนาด 3×3 ตัดหลักที่ทำให้เกิดเกิรธ 6 ในที่นี้เลือกหลักที่ 1 ของทุกๆเมทริกซ์ย่อย

$$\mathbf{H}_{\text{full rank}} = \left[\begin{array}{c|cc|c|cc|c|cc|c|cc} & 2 & 4 & & 16 & 32 & & 27 & 54 & \cdots & & 76 & 51 \\ & 4 & 8 & & 32 & 64 & & 54 & 7 & \cdots & & 51 & 1 \\ & 8 & 16 & & 64 & 27 & & 7 & 14 & \cdots & & 1 & 2 \end{array}\right]$$

จากนั้นเลือกหลักที่เหลือจำนวน 6 หลัก ในตัวอย่างนี้จะเลือกแบบเรียงติดกันจาก $H_{\text{full rank}}$ จะได้เมทริกซ์ตรวจสอบพาริตี้สำหรับอัตรารหัสเท่ากับ 0.5 เป็น

$$\mathbf{H}_{\text{Code rate=0.5}} = \begin{bmatrix} 2 & 4 & 16 & 32 & 27 & 54 \\ 4 & 8 & 32 & 64 & 54 & 7 \\ 8 & 16 & 64 & 27 & 7 & 14 \end{bmatrix}_{3p \times 6p}$$

หากเลือกตัดหลักที่ 2 ของทุกๆเมทริกซ์ย่อยและเลือกหลักจาก $\mathbf{H}_{\text{full rank}}$ แบบเรียงติดกัน จะได้เมทริกซ์ตรวจสอบพาริตี้สำหรับอัตรารหัสเท่ากับ 0.5 เป็น

$$\mathbf{H}_{\text{full rank}} = \left[\begin{array}{c|c|cc|c|cc|c|cc|c|c} 1 & & 4 & 8 & & 32 & 64 & & 54 & \cdots & 38 & & 51 \\ 2 & & 8 & 16 & & 64 & 27 & & 7 & \cdots & 76 & & 1 \\ 4 & & 16 & 32 & & 27 & 54 & & 14 & \cdots & 51 & & 2 \end{array}\right]$$

$$\mathbf{H}_{\text{Code rate=0.5}} = \begin{bmatrix} 1 & 4 & 8 & 32 & 64 & 54 \\ 2 & 8 & 16 & 64 & 27 & 7 \\ 4 & 16 & 32 & 27 & 54 & 14 \end{bmatrix}_{3p \times 6p}$$

เช่นเดียวกัน หากเลือกตัดหลักที่ 3 ของทุกๆเมทริกซ์ย่อยและเลือกหลักที่เหลือแบบเรียงติดกัน เมทริกซ์ตรวจสอบพาริตี้สำหรับอัตรารหัสเท่ากับ 0.5 มีค่าเป็น

$$\mathbf{H}_{\text{full rank}} = \left[\begin{array}{cc|cc|cc|c|cc} 1 & 2 & 8 & 16 & 64 & 27 & \cdots & 38 & 76 \\ 2 & 4 & 16 & 32 & 27 & 54 & \cdots & 76 & 51 \\ 4 & 8 & 32 & 64 & 54 & 7 & \cdots & 51 & 1 \end{array}\right]$$

$$\mathbf{H}_{\text{Code rate=0.5}} = \begin{bmatrix} 1 & 2 & 8 & 16 & 64 & 27 \\ 2 & 4 & 16 & 32 & 27 & 54 \\ 4 & 8 & 32 & 64 & 54 & 7 \end{bmatrix}_{3p \times 6p}$$

นอกจากนี้ วิธีการออกแบบนี้ไม่จำเป็นที่จะต้องเรียงหลักติดกัน การออกแบบบางครั้งสามารถเลือกหลักจากบล็อกย่อยไม่ติดกันได้ ตัวอย่างเช่น เลือกตัดหลักที่ 3 ทุกๆบล็อกย่อยและหลักที่นำมาต่อกันในบล็อกที่ 1, บล็อกที่ 3 และบล็อกสุดท้าย ได้เมทริกซ์ตรวจสอบพาริตี้ดังนี้

$$\mathbf{H}_{\text{Code rate=0.5}} = \begin{bmatrix} 1 & 2 & 64 & 27 & 38 & 76 \\ 2 & 4 & 27 & 54 & 76 & 51 \\ 4 & 8 & 54 & 7 & 51 & 1 \end{bmatrix}_{3p \times 6p}$$

จากวิธีการออกแบบเมทริกซ์ตรวจสอบพาริตี้เพื่อให้ได้เกิรธเท่ากับ 8 ที่ได้นำเสนอนี้สามารถสรุปค่าพารามิเตอร์ต่าง ๆ ในการออกแบบดังตารางที่ 4.1

ตารางที่ 4.1 ค่าพารามิเตอร์ในออกแบบสำหรับรหัสควอไซไซคลิคแอลดีพีซีและได้เกิรธเท่ากับ 8

j	k	p	$j \times p$	$k \times p$	element a	Girth-6	Girth-8	Girth-10
3	5	47	141	235	5	0%	100%	0%
3	5	61	183	305	2	0%	100%	0%
3	5	101	303	505	2	0%	100%	0%
3	5	151	453	755	7	0%	100%	0%
3	5	601	1,803	3,005	7	0%	100%	0%
3	5	701	2,103	3,505	7	0%	100%	0%
3	6	67	201	402	2	0%	100%	0%
3	6	71	213	426	7	0%	100%	0%
3	6	83	249	498	2	0%	100%	0%
3	6	101	303	606	2	0%	100%	0%
3	6	107	321	642	2	0%	100%	0%

3	6	211	633	1,266	2	0%	100%	0%
3	9	293	879	2,637	2	0%	100%	0%
3	9	313	939	2,817	17	0%	100%	0%
3	9	601	1,803	5,409	7	0%	100%	0%
3	10	311	933	3,110	17	0%	100%	0%
3	10	401	1,203	4,010	3	0%	100%	0%
3	12	599	1,797	7,188	7	0%	100%	0%
3	12	601	1,803	7,212	7	0%	100%	0%
3	12	797	2,391	9,564	2	0%	100%	0%
3	15	701	2,103	10,515	2	0%	100%	0%
3	15	811	2,433	12,165	3	0%	100%	0%
3	15	1,021	3,063	15,315	3	0%	100%	0%
3	16	709	2,137	11,344	2	0%	100%	0%
3	17	797	2,391	13,549	2	0%	100%	0%
3	17	907	2,712	15,419	17	0%	100%	0%
3	17	929	2,787	15,793	3	0%	100%	0%
3	17	1,069	3,027	18,173	7	0%	100%	0%
3	18	1,553	4,659	27,954	3	0%	100%	0%
3	18	1,801	5,403	32,418	11	0%	100%	0%

จากตารางที่ 4.1 การสร้างเมทริกซ์พาริตี้อยู่ในช่วงอัตรารหัสตั้งแต่ 0.4 ถึง 0.83 และมีข้อสังเกตุคือ อัตรารหัสที่มากขึ้นจะต้องให้ขนาดของเมทริกซ์หมุนสลับตำแหน่งจะมีขนาดที่ใหญ่ขึ้นตาม ทั้งนี้เพื่อไม่ให้เกิดเกิรธ 6 ในการสร้าง อีกทั้งการออกแบบสามารถในแต่ละอัตรารหัสทำได้บางค่าของขนาดของเมทริกซ์หมุนสลับตำแหน่ง ดังนั้นหากการออกแบบที่ต้องการพารามิเตอร์ที่แตกต่างจากนี้ออกไปและต้องการให้เมทริกซ์ที่ได้มีเกิรธมากกว่า 6 ขึ้นไปต้องเปลี่ยนลำดับในการเลือกหลักที่นำมาต่อกัน ซึ่งจะได้กล่าวถึงในหัวข้อถัดไป

4.3 การออกแบบรหัสควอไซไซคลิคแอลดีพีซีเพื่อให้ได้เกิรธตั้งแต่ 8 ขึ้นไป

จากหัวข้อที่ 4.1 เป็นการออกแบบเมทริกซ์ตรวจสอบพาริตี้เต็มจำนวน $\mathbf{H}_{\text{full rank}}$ ที่มีเกิรธเท่ากับ 6 และนำหลักที่เหลือมาต่อกัน แต่ทั้งนี้วิธีการดังกล่าวยังไม่ครอบคลุมถึงการออกแบบต่อขนาดของเกิรธที่มากกว่า 8 และไม่ครอบคลุมต่อขนาดของเมทริกซ์หมุนสลับตำแหน่งบางค่า ดังนั้นเพื่อให้สามารถออกแบบเมทริกซ์ตรวจสอบพาริตี้ให้ครอบคลุมต่อความต้องการ วิธีที่จะเสนอต่อไปนี้จะใช้วิธีการค้นหาหลักของ $\mathbf{H}_{\text{full rank}}$ ที่เหมาะสม โดยจะเรียงหลักต่อกันเข้าไปทีละหลักและทำการ

ตรวจสอบเกิรธที่ได้ว่ามีขนาดตามที่ต้องการ หากหลักที่นำมาต่อกันได้ขนาดเกิรธตามต้องการจะทำการเก็บเมทริกซ์ชุดนั้นไว้และนำหลักใน $\mathbf{H}_{\text{full rank}}$ เลือกมาเรียงต่อกันไป แต่หากหลักที่นำมาต่อกันไม่ได้เกิรธตามต้องการจะไม่นำหลักดังกล่าวเข้ามารวมในเมทริกซ์ตรวจสอบพาริตี้ พิจารณาตัวอย่างการออกแบบโดยการใช้คำนวณในการค้นหาได้ดังตัวอย่างต่อไปนี้

ตัวอย่างที่ 4.4 การออกแบบรหัสควอไซไซคลิคแอลดีพีซี ที่อัตรารหัส 0.4, น้ำหนัก 1 ในแนวตั้ง j เท่ากับ 3, น้ำหนัก 1 ในแนวนอน k เท่ากับ 5 และขนาดเมทริกซ์หมุนสลับตำแหน่ง p เท่ากับ 31 ได้อิลิเมนต์ a เท่ากับ 3 ที่สามารถสร้างเมทริกซ์เต็มจำนวน (Full Rank) ขนาด $3p\times 30p$ ดังนั้นเมทริกซ์เต็มจำนวนคือ

$$\mathbf{H}_{\text{full rank}}=\begin{bmatrix} 1 & 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & \cdots & \cdots & 23 & 7 & 21 \\ 3 & 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & \cdots & \cdots & 7 & 21 & 1 \\ 9 & 27 & 19 & 26 & 16 & 17 & 20 & 29 & 25 & 13 & \cdots & \cdots & 21 & 1 & 3 \end{bmatrix}_{3p\times 30p}$$

หากทำการออกแบบด้วยวิธีการในหัวข้อที่ 4.2 โดยเลือกตัดหลักที่ 3 ของทุกบล็อกย่อยขนาด 3×3 จะได้เมทริกซ์ตรวจสอบพาริตี้เป็น

$$\mathbf{H}_{\{1,2,4,5,7\}}=\begin{bmatrix} 1 & 3 & 27 & 19 & 16 \\ 3 & 9 & 19 & 26 & 20 \\ 9 & 27 & 26 & 16 & 29 \end{bmatrix}_{3p\times 5p}$$

เมื่อทำการนับจำนวนเกิรธของเมทริกซ์ตรวจสอบพาริตี้ $\mathbf{H}_{\{1,2,4,5,7\}}$ แล้ว พบว่ามีโกลบอลเกิรธมีค่าเท่ากับ 6 โดยแบ่งเป็นโลคอลเกิรธ 6 เท่ากับ 60% และโลคอลเกิรธ 8 เท่ากับ 40% ดังนั้นการออกแบบเพื่อให้ได้เกิรธ 8 จำเป็นต้องเปลี่ยนวิธีการออกแบบ โดยการเลือกหลักที่นำมาต่อกันใหม่หมด

ขั้นตอนแรกในการออกแบบให้ทำการเลือกหลักที่อยู่ติดกัน 3 หลักจาก $\mathbf{H}_{\text{full rank}}$ ในที่นี้คือหลักที่ 1, 2 และ 3

$$\mathbf{H}_{\{1,2,3\}}=\begin{bmatrix} 1 & 3 & 9 \\ 3 & 9 & 27 \\ 9 & 27 & 19 \end{bmatrix}$$

จากนั้นทำการตรวจสอบเกิรธที่ได้ หากเกิรธที่ได้ตรงตามเกิรธที่ต้องการให้เก็บเมทริกซ์ชุดนี้ไว้และนำหลักต่อไปนำมาต่อ หากไม่ใช่ให้นำหลักสุดท้ายที่นำมาต่อออกไปและนำหลักจาก $\mathbf{H}_{\text{full rank}}$

ถัดไปเข้ามาต่อแทน ในขั้นตอนแรก $\mathbf{H}_{\{1,2,3\}}$ ได้เกิรธเท่ากับ 6 ดังนั้นให้นำหลักที่ 3 ออกไปและนำหลักที่ 4 มาใส่แทน

$$\mathbf{H}_{\{1,2,4\}} = \begin{bmatrix} 1 & 3 & 27 \\ 3 & 9 & 19 \\ 9 & 27 & 26 \end{bmatrix}$$

เมทริกซ์ชุดใหม่ที่ได้นี้เมื่อตรวจสอบเกิรธแล้ว พบว่าเกิรธที่ได้มีค่าเท่ากับ 10 ดังนั้นให้เก็บเมทริกซ์ $\mathbf{H}_{\{1,2,4\}}$ ไว้ จากนั้นนำหลักถัดไปจาก $\mathbf{H}_{\text{full rank}}$ คือหลักที่ 5 เข้ามาต่อ จะได้

$$\mathbf{H}_{\{1,2,4,5\}} = \begin{bmatrix} 1 & 3 & 27 & 19 \\ 3 & 9 & 19 & 26 \\ 9 & 27 & 26 & 16 \end{bmatrix}$$

ทำการตรวจสอบเกิรธของเมทริกซ์ $\mathbf{H}_{\{1,2,4,5\}}$ พบว่าเกิรธที่ได้มีค่าเท่ากับ 8 ให้เก็บเมทริกซ์ $\mathbf{H}_{\{1,2,4,5\}}$ ไว้ จากนั้นนำหลักถัดไปคือหลักที่ 5 เข้ามาต่อในหลักถัดไป

$$\mathbf{H}_{\{1,2,4,5,6\}} = \begin{bmatrix} 1 & 3 & 27 & 19 & 26 \\ 3 & 9 & 19 & 26 & 16 \\ 9 & 27 & 26 & 16 & 17 \end{bmatrix}$$

ตรวจสอบเกิรธของเมทริกซ์ $\mathbf{H}_{\{1,2,4,5,6\}}$ พบว่าเกิรธที่ได้มีค่าเท่ากับ 6 และหากสังเกตุจะพบว่าเมทริกซ์ชุดนี้มีค่าสำหรับเมทริกซ์หมุนสลับตำแหน่งที่มีค่าเท่ากับ 26 ซ้ำกัน 3 ค่า และค่าดังกล่าวอยู่ในทุกหลักและทุกแถวซึ่งเป็นรูปแบบที่ทำให้เกิดเกิรธ 6 ดังนั้นหลักที่ 6 จึงไม่ใช่หลักที่จะสร้างเมทริกซ์ที่จะทำให้ได้เกิรธ 8 จากวิธีการที่ได้นำเสนอมานี้ให้ทำซ้ำเช่นนี้ไปเรื่อยๆจนกว่าจะพบหลักที่สามารถสร้างเกิรธ 8 ได้ จากตัวอย่างนี้หลักที่นำมาต่อที่จะทำให้ได้เกิรธ 8 คือหลักที่ 10 ดังนั้นเมทริกซ์ตรวจสอบพาริตี้ที่ได้คือ

$$\mathbf{H}_{\{1,2,4,5,10\}} = \begin{bmatrix} 1 & 3 & 27 & 19 & 29 \\ 3 & 9 & 19 & 26 & 25 \\ 9 & 27 & 26 & 16 & 13 \end{bmatrix}_{3p \times 5p}$$

จากเมทริกซ์ $\mathbf{H}_{\{1,2,4,5,10\}}$ เป็นหนึ่งในรูปแบบที่สามารถสร้างเมทริกซ์ตรวจสอบพาริตี้ให้ได้เกิรธ 8 นอกจากวิธีการนี้สามารถเปลี่ยนค่าเมทริกซ์หมุนสลับตำแหน่งทั้งหมดโดยการเลื่อน

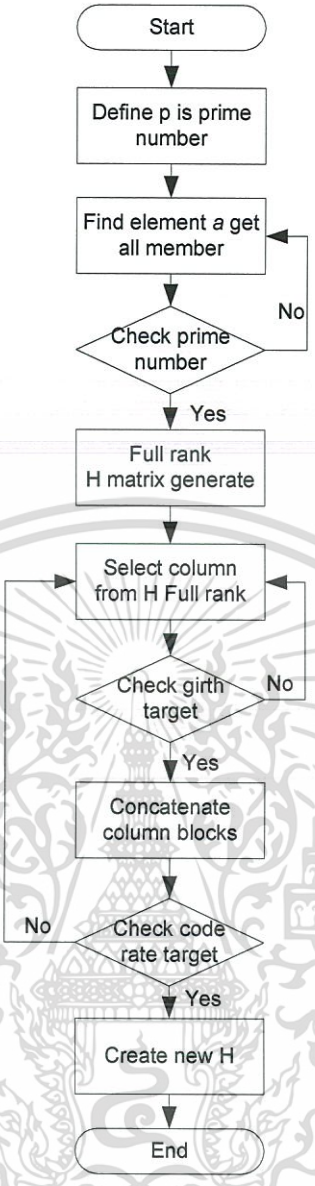
เช่น ลำดับที่ได้ในการสร้างคือ $\{1,2,4,5,10\}$ ต้องการเมทริกซ์ในหลักแรกเริ่มต้นในหลักที่ 4 จาก $\mathbf{H}_{\text{full rank}}$ ดังนั้นเมทริกซ์ชุดใหม่ที่ คือ $(4-1)+\{1,2,4,5,10\}=\{4,5,7,8,13\}$ จะได้ $\mathbf{H}_{\{4,5,7,8,13\}}$

$$\mathbf{H}_{\{4,5,7,8,13\}} = \begin{bmatrix} 27 & 19 & 16 & 17 & 8 \\ 19 & 26 & 17 & 20 & 24 \\ 26 & 16 & 20 & 29 & 10 \end{bmatrix}_{3p\times 5p}$$

จากตัวอย่างที่ 4.4 วิธีการนี้สามารถนำไปใช้ในการสร้างเมทริกซ์ตรวจสอบพาริตี้ได้ทุกค่าเกิรธ 6, 8, 10 และ 12 และการออกแบบด้วยวิธีนี้สามารถสรุปขั้นตอนการออกแบบได้ดังนี้

- ขั้นตอนแรกกำหนดขนาดเมทริกซ์หมุนสลับตำแหน่งต้องเป็นเลขจำนวนเฉพาะ
- ขั้นตอนที่สองให้คำนวณหาค่าอิลิเมนต์ a ที่ทำให่เกิดของสมาชิกทั้งหมดที่ไม่ซ้ำกันด้วยการมอดูโลเพื่อสร้างเมทริกซ์เต็มจำนวน
- ขั้นตอนที่สามเลือกค่าอิลิเมนต์ a ที่เป็นเลขจำนวนเฉพาะ
- ขั้นตอนที่สี่สร้างเมทริกซ์ตรวจสอบพาริตี้เต็มจำนวน ในขั้นตอนนี้จะปราศจากไซเคิล 4 และมีเกิรธอย่างน้อยเท่ากับ 6
- ขั้นที่ห้านำหลักจากเมทริกซ์เมทริกซ์ตรวจสอบพาริตี้เต็มจำนวนมาต่อรวมกันและตรวจสอบว่ายังได้เกิรธที่ต้องการรึไม่
- ขั้นตอนสุดท้ายว่าได้อัตรารหัสที่ต้องการรึไม่ หากสามารถสร้างเมทริกซ์ตรวจสอบพาริตี้และได้อัตรารหัสที่ต้องการก็สามารถนำเมทริกซ์ชุดนี้ไปใช้งานต่อไป แต่หากสร้างไม่ได้ต้องทำการเพิ่มขนาดของเมทริกซ์หมุนสลับตำแหน่งหรือเพิ่มค่า p จากนั้นกระบวนออกแบบใหม่อีกครั้งจากขั้นตอนแรก

จากสรุปขั้นตอนในการสร้างเมทริกซ์ตรวจสอบพาริตี้สามารถเขียนให้อยู่ในรูปของโฟลชาร์ตได้ดังรูปที่ 4.4



รูปที่ 4.4 โฟลชาร์ตขั้นตอนการออกแบบเมทริกซ์ตรวจสอบพาริตี้

4.4 การลดขั้นตอนออกแบบรหัสดีพีซีเพื่อให้ได้เกิรธมากกว่า 8

จากการออกแบบที่ได้นำเสนอมาแล้วในหัวข้อที่ 4.3 เป็นการออกแบบรหัสแอลดีพีซีเพื่อให้ได้เมทริกซ์ตรวจสอบพาริตี้มีขนาดของเกิรธมากกว่า 8 ใช้การตรวจสอบเรียงจากหลักแรกไปเรื่อยๆ ซึ่งหากเมทริกซ์ที่ต้องการออกแบบเป็นเมทริกซ์ที่มีขนาดใหญ่การคำนวณค้นหาหลักที่ต้องการจะใช้เวลามากขึ้น ดังนั้นเพื่อลดเวลาในการค้นหาวิธีการสามารถมองข้ามบางหลักโดยไม่ตองนำมาคิดได้ หากพิจารณาจากตัวอย่างที่ 4.4 จะพบว่าทุกๆบล็อกย่อยขนาด 3×3 จะมีอยู่ 1 หลักที่ทำให้เกิดเกิรธ 6 ซึ่งได้อธิบายไว้แล้วในหัวข้อที่ 4.2 ดังนั้นหากทำการตัดหลักใดหลักหนึ่งจากบล็อกย่อยขนาด 3×3 ทุกๆบล็อกขนาดของเมทริกซ์ที่จะนำไปใช้ในการเลือกหลักมาต่อกันเพื่อเมทริกซ์พาริตี้ชุดใหม่จะ

ลดเหลือเพียง 2 ใน 3หรือก็คือวิธีการนี้หลักการแบบเดียวกันกับวิธีการออกแบบจากเกิรธ 6 เป็น 8 จากนั้นทำการสร้างเมทริกซ์พาริตี้ตามวิธีการที่ได้นำเสนอมาแล้วในหัวข้อที่ 4.3

ตัวอย่างลำดับที่สามารถสร้างเมทริกซ์ตรวจสอบพาริตี้เพื่อให้ได้ขนาดของเกิรธเท่ากับ 10 คือ $i=\{1,2,4,16,64,128\}$ เมื่อกำหนดให้ i คือตำแหน่งของหลักจากเมทริกซ์เต็มจำนวน ได้พารามิเตอร์ในการสร้างดังตารางที่ 4.2

ตารางที่ 4.2 ค่าพารามิเตอร์ในออกแบบสำหรับรหัสควอไซไซคลิคแอลดีพีซีและได้เกิรธเท่ากับ 10

j	k	p	$j\times p$	$k\times p$	element a	Girth-8	Girth-10	Girth-12
3	6	547	1,641	3,282	2	0%	100%	0%
3	6	641	1,923	3,846	3	0%	100%	0%
3	6	701	2,103	4,206	2	0%	100%	0%
3	6	857	2,571	5,142	3	0%	100%	0%
3	6	911	2,733	5,466	17	0%	100%	0%

และตัวอย่างลำดับที่สามารถสร้างเมทริกซ์ตรวจสอบพาริตี้เพื่อให้ได้ขนาดของเกิรธเท่ากับ 12 คือ $i=\{1,2,4,16,256\}$ สำหรับรหัสแอลดีพีซี (3, 5) และ $i=\{1,2,4,16,256,1024\}$ สำหรับรหัสแอลดีพีซี (3, 6) โดยเมทริกซ์หมุนสลับตำแหน่ง p ของทั้งสองแบบจะต้องมีค่ามากกว่า ค่าของสูงสุดของ i หรือ $p>i$ และได้พารามิเตอร์ในการสร้างดังตารางที่ 4.3

ตารางที่ 4.3 ค่าพารามิเตอร์ในออกแบบสำหรับรหัสควอไซไซคลิคแอลดีพีซีและได้เกิรธเท่ากับ 12

j	k	p	$j\times p$	$k\times p$	element a	Girth-8	Girth-10	Girth-12
3	5	601	1,803	3,005	7	0%	0%	100%
3	5	991	2,973	4,955	7	0%	0%	100%
3	6	1,901	5,703	11,406	2	0%	0%	100%

4.3 ผลการทดลองเปรียบเทียบสมรรถนะของรหัสแอลดีพีซี

จากการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ได้เสนอไว้ข้างต้นในบทนี้ ในหัวข้อนี้จะทำการทดสอบสมรรถนะของรหัสเปรียบเทียบกับการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่มีโครงสร้างต่าง ๆ ที่ได้นำกล่าวถึงมาแล้วทั้งหมดกับเมทริกซ์ตรวจสอบพาริตี้ในงานวิจัยนี้และใช้การถอดรหัสแอลดีพีซีแบบล็อก-รวมผลคูณบนช่องสัญญาณเกาส์เซียนโดยกล้ำสัญญาณแบบ BPSK ในแต่อัตรารหัสดังตารางที่ 4.4 โดยทดสอบภายใต้ตัวแปรดังตารางที่ 4.5 ถึง 4.11

ตารางที่ 4.4 การทดสอบสมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสค่าต่าง ๆ

อัตรารหัส	ขั้นตอนการทดสอบ
0.4	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีที่ออกแบบด้วยวิธีการของ Tanner กับรหัสควอไซไซคลิคแอลดีพีซีที่ออกแบบด้วยวิธีการออกแบบของผู้วิจัย รวมทั้งเปรียบเทียบกับรหัสแอลดีพีซีที่ออกแบบด้วยอัลกอริทึมพีอีจี
0.4	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีที่ด้วยกันที่สามารถออกแบบเพื่อสร้างเกิรธขนาดมากกว่า 6 กับรหัสควอไซไซคลิคแอลดีพีซีที่นำเสนอในวิทยานิยนธ์นี้
0.5	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของวิทยานิพนธ์นี้ที่มีน้ำหลักหลักเท่ากับ 3 และมีเกิรธเท่ากับ 8 กับการออกแบบรหัสแอลดีพีซีที่มีน้ำหลักหลักมากกว่า 3 ซึ่งในที่นี้คือ รหัสบล็อคไม่สมบูรณ์แบบสมดุลย์
0.5	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยด้วยกันเอง โดยเปรียบเทียบเมทริกซ์ตรวจสอบพาริตี้ที่มีขนาดของเกิรธเท่ากับ 6, 8 และ 10
0.7	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยนี้ กับรหัสอาร์เรย์, รหัสอาร์เรย์แบบปรับปรุงและรหัสควอไซไซคลิคแอลดีพีซีแบบสุ่มค่าให้กับเมทริกซ์หมุนสลับตำแหน่ง
0.75	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยนี้ กับรหัสควอไซไซคลิคแอลดีพีซีแบบ Tanner ที่กำหนดค่าอิลิเม้นต์ด้วยการหาเซทร่วม และเปรียบเทียบเทียบกับรหัสแอลดีพีซีที่สร้างเกิรธขนาดใหญ่ด้วยอัลกอริทึมพีอีจี
0.82	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยนี้โดยมีระยะห่างต่ำสุดไม่เกิน 24 กับรหัสเรขาคณิตยูคลิดทีมีระยะห่างต่ำสุดเท่ากับ 65
0.9	เปรียบเทียบระหว่างรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยนี้ ที่มี Cloumn weigth ที่แตกต่างกัน

ตารางที่ 4.5 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีอัตรารหัสประมาณ 0.4

Type	Code	m	n	j	k	p	Girth	Iteration
PEG	0.4	2,253	3,755	3	5	-	12	20
QC Proposed	0.4	2,253	3,755	3	5	751	8	20
QC	0.4	2,253	3,755	3	5	751	6	20

กำหนดให้ m คือ จำนวนแถวของเมทริกซ์ตรวจสอบพาริตี้

n คือ จำนวนหลักของเมทริกซ์ตรวจสอบพาริตี้

j คือ น้ำหนัก 1 ในแนวตั้ง หรือ จำนวน “1” ในแถวของเมทริกซ์ตรวจสอบพาริตี้

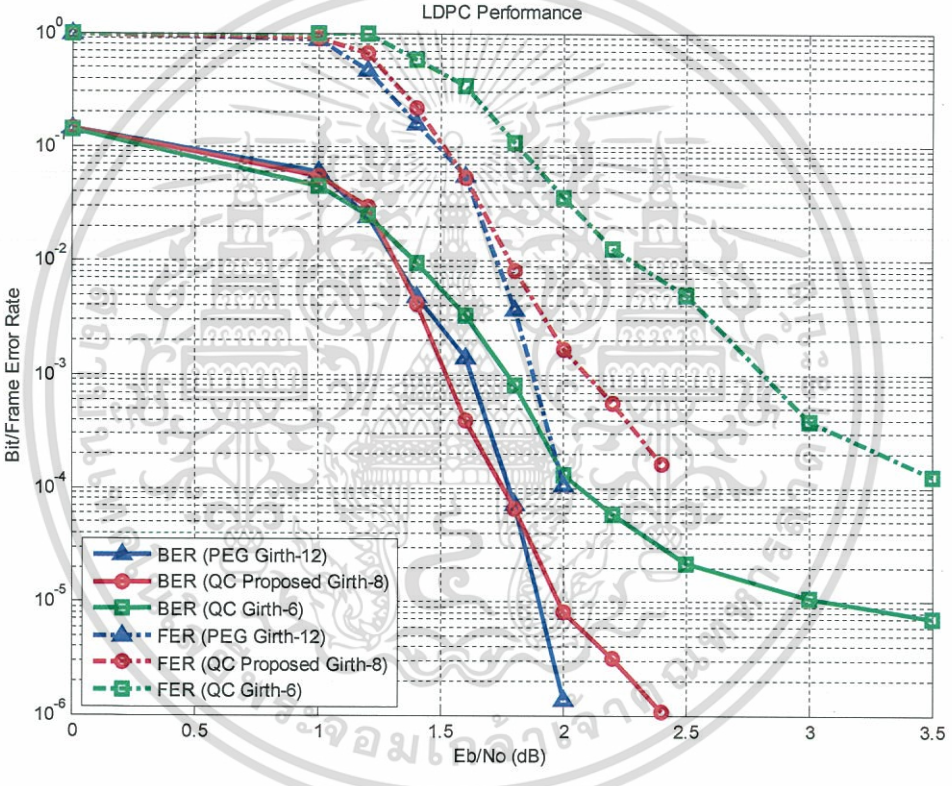
k คือ น้ำหนัก 1 ในแนวนอน จำนวน “1” ในหลักของเมทริกซ์ตรวจสอบพาริตี้

p คือ ขนาดของเมทริกซ์หมุนสลับตำแหน่ง

Girth คือขนาดของโกลบอลเกิรธที่ได้จากเมทริกซ์ตรวจสอบพาริตี้

Iteration คือ จำนวนรอบการถอดรหัส

จากตารางที่ 4.5 เป็นการทดสอบสมรรถนะของรหัสควอไซไซคลิคแอลดีพีซี [13] ที่มีขนาดของเกิรธเท่ากับ 6 และรหัสควอไซไซคลิคแอลดีพีซีของงานวิจัยนี้ที่มีขนาดของเกิรธ 8 และยังเปรียบกับรหัสแอลดีพีซีที่ออกแบบด้วยอัลกอริทึมพีอีซีที่มีขนาดเกิรธเท่ากับ 12 และกำหนดให้รอบวนซ้ำในขั้นตอนการถอดรหัสเท่ากับ 20 รอบ ผลที่ได้จากการทดสอบสมรรถนะอยู่ในรูปแบบของอัตราบิตผิดพลาดหรือ BER และอัตราเฟรมผิดพลาดหรือ FER เทียบกับ Eb/No ดังรูปที่ 4.5



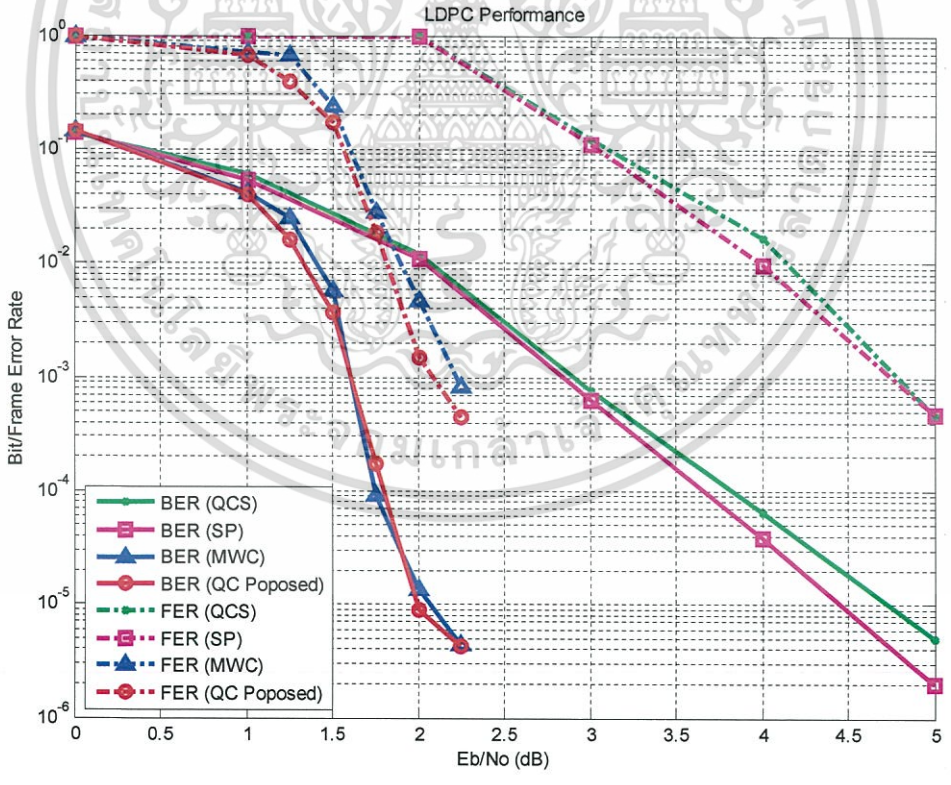
รูปที่ 4.5 สมรรถนะของรหัสแอลดีพีซีอัตรารหัสประมาณ 0.4

จากรูปที่ 4.5 แสดงให้เห็นถึงสมรรถนะของรหัสควอไซไซคลิคแอลดีพีซีที่มีขนาดเกิรธเท่ากับ 8 สามารถแก้ไขข้อมูลผิดพลาดได้ดีกว่ารหัสควอไซไซคลิคแอลดีพีซีที่มีขนาดเกิรธเท่ากับ 6 อย่างมาก และเมื่อเปรียบเทียบรหัสควอไซไซคลิคแอลดีพีซีที่มีขนาดเกิรธเท่ากับ 8 กับวิธีการออกแบบรหัสแอลดีพีซีที่ใช้อัลกอริทึมพีอีจีที่มีเกิรธเท่ากับ 12 สมรรถนะต่างกันอยู่ประมาณ 0.4 dB ทั้งอัตราบิตผิดพลาดและอัตราเฟรมผิดพลาด ทั้งนี้เนื่องจากจำนวนเกิรธที่แตกต่างกันระหว่างเกิรธ 8 และ 12 ซึ่งส่งผลต่อสมรรถนะโดยรวม

ในการทดสอบสมรรถนะของรหัสแอลดีพีซีต่อไปจะทดสอบด้วยวิธีการที่ออกแบบรหัสแอลดีพีซีที่มีขนาดของเกิรธเท่ากับ 8 เหมือนกันโดยเป็นการออกแบบบนโครงสร้างควอไซไซคลิคทั้งหมด ซึ่งประกอบด้วยวิธีการของวิจัยนี้เปรียบเทียบกับวิธีการออกแบบของ [16] และมีวิธีการออกแบบย่อยออกไปอีก 3 แบบและได้อธิบายวิธีการออกแบบทั้งหมดไว้แล้วในบทที่ 3 การทดสอบต่อไปนี้ใช้พารามิเตอร์ในการสร้างเมทริกซ์ตรวจสอบพาริตี้ดังตารางที่ 4.6 และสมรรถนะของรหัสแอลดีพีซีที่ได้ดังรูปที่ 4.6

ตารางที่ 4.6 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีระหว่าง QCS, SP, MWC และ QC ของงานวิจัยนี้ที่อัตรารหัสเท่ากับ 0.4

Type	Code	m	n	j	k	p	Girth	Iteration
QC QCS	0.4	2,253	3,755	3	5	751	8	20
QC SP	0.4	2,253	3,755	3	5	751	8	20
QC MWC	0.4	2,253	3,755	3	5	751	8	20
QC Proposed	0.4	2,253	3,755	3	5	751	8	20



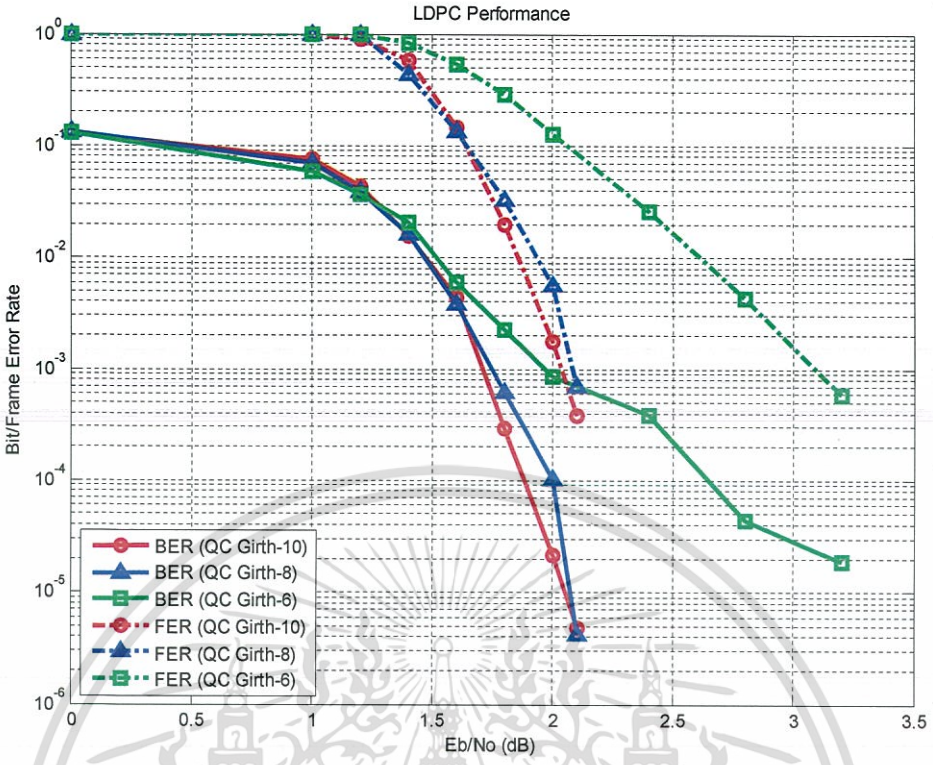
รูปที่ 4.6 สมรรถนะของรหัสแอลดีพีซีระหว่าง QCS, SP, MWC และ QC ของงานวิจัยนี้ที่อัตรารหัสเท่ากับ 0.4

จากรูปที่ 4.6 ผลที่ได้แสดงให้เห็นถึงสมรรถนะของรหัสแอลดีพีซีที่ได้นำเสนอในงานวิจัยนี้เหนือกว่าวิธีการออกแบบ QCS และ SP ประมาณ 2.5 dB ในเงื่อนไขจากตารางที่ 4.6 และให้ผลที่ใกล้เคียงกันกับวิธีการออกแบบ MWC ทั้งนี้เมื่อพิจารณาระยะห่างต่ำสุดของวิธีการออกแบบย่อยทั้ง 3 แบบ วิธีการออกแบบ MWC มีระยะห่างต่ำสุดประมาณ 24 ซึ่งเป็นระยะห่างต่ำสุดที่มีค่าสูงสุด ส่วนวิธีการออกแบบ QCS และ SP มีค่าประมาณ 14 เมื่อพิจารณาผลที่ได้จากการออกแบบที่ได้นำเสนอที่ได้สมรรถนะเทียบเท่าวิธีการออกแบบ MWC เนื่องจากระยะห่างต่ำสุดรหัสแอลดีพีซีที่ได้นำเสนอในงานวิจัยนี้มีค่าประมาณ 24 เช่นเดียวกัน จากผลที่ได้ทั้งหมดจึงสรุปได้ว่าเมทริกซ์ตรวจสอบพาริตี้ที่มีขนาดของเมทริกซ์และเกิรธที่เท่ากันบางครั้งผลที่ได้อาจแตกต่างกันเนื่องจากระยะห่างต่ำสุดที่แตกต่างกัน แต่ทั้งนี้การหาค่าระยะห่างต่ำสุดของรหัสแอลดีพีซีในหลายๆวิธี (ยกเว้น รหัสเรขาคณิตยูคลิด และ รหัสเรขาคณิตเชิงฉายภาพ) ไม่สามารถที่จะคำนวณหาค่านี้ได้โดยตรง การจะหาค่าระยะห่างต่ำสุดได้นั้นจะต้องทำการจำลองการทำงาน [27] ด้วยการสร้างแพทเทิร์นในการทดสอบและเก็บผลของระยะห่างต่ำสุดที่ได้และค่าที่ได้เป็นเพียงค่าโดยประมาณเท่านั้น

ในการทดสอบต่อไปนี้จะทำการทดสอบรหัสแอลดีพีซีที่อัตรารหัส 0.5 โดยทำการทดสอบสมรรถนะเปรียบเทียบกับการออกแบบเมทริกซ์ตรวจสอบพาริตี้ที่ได้เสนอของงานวิจัยนี้ด้วยใช้โครงสร้างควอไซไซคลิคที่มีขนาดของเกิรธเท่ากับ 6, 8 และ 10 และมีพารามิเตอร์ในการออกแบบดังตารางที่ 4.7 และผลการทดสอบสมรรถนะที่ได้ดังรูปที่ 4.7

ตารางที่ 4.7 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่มีขนาดของเกิรธเท่ากับ 6, 8 และ 10 ที่อัตรารหัสเท่ากับ 0.5

Type	Code rate	m	n	j	k	p	Girth	Iteration
QC	0.5	1,641	3,282	3	6	574	6	20
QC	0.5	1,641	3,282	3	6	574	8	20
QC	0.5	1,641	3,282	3	6	574	10	20



รูปที่ 4.7 สมรรถนะของรหัสแอลดีพีซีที่มีขนาดของเกิรธเท่ากับ 6, 8 และ 10 ที่อัตรารหัสเท่ากับ 0.5

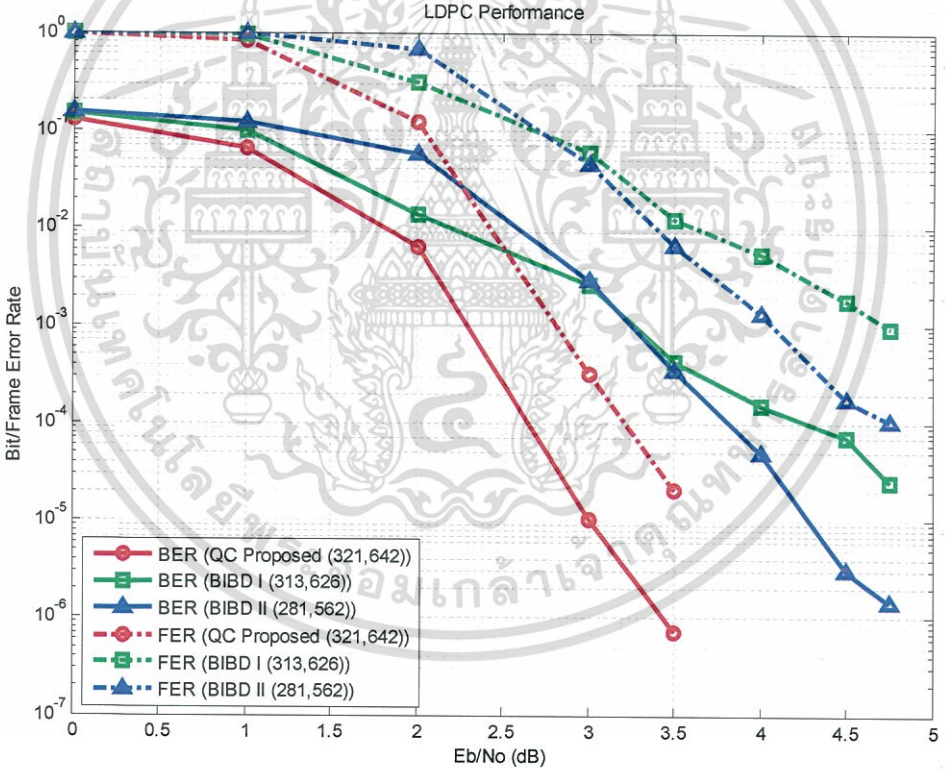
ผลการทดลองในรูปที่ 4.7 พบว่ารหัสแอลดีพีซีที่มีขนาดของเกิรธมากกว่า 6 มีสมรรถนะที่เหนือกว่ารหัสแอลดีพีซีที่มีขนาดของเกิรธเท่ากับ 6 อยู่ประมาณ 1.25 dB เมื่อพิจารณาเมทริกซ์ตรวจสอบพาริตี้ที่มีขนาดเท่ากันทุกประการรวมทั้งค่าระยะห่างต่ำสุดหากเทียบเท่ากันแล้ว สมรรถนะที่ได้จะขึ้นกับขนาดของเกิรธ แต่เมื่อพิจารณาระหว่างเกิรธ 8 และเกิรธ 10 ในการทดสอบนี้ในส่วนของอัตราบิตผิดพลาดหรือ BER ไม่แตกต่างกันมากแต่อัตราเฟรมผิดพลาดหรือ FER นั้น เมทริกซ์ที่มีขนาดของเกิรธ เท่ากับ 10 สามารถแก้ไขข้อมูลผิดพลาดให้ถูกต้องทุกบิตในเฟรมนั้นๆได้ดีกว่า ทั้งนี้การทดสอบนี้กำหนดค่ารอบการทำงานในการถอดรหัสคงที่ไว้ที่ 20 รอบ การเพิ่มรอบการถอดรหัสน่าจะส่งผลต่อสมรรถนะโดยรวมของรหัสแอลดีพีซีให้ดียิ่งขึ้น โดยเฉพาะรหัสแอลดีพีซีที่มีขนาดเกิรธที่ใหญ่

นอกจากการทดสอบรหัสแอลดีพีซีที่อัตรารหัส 0.5 ในผลการทดสอบก่อนหน้านี้รหัสแอลดีพีซีของงานวิจัยที่นำเสนอนี้กำหนดให้ “1” ในแต่ละหลักในเมทริกซ์มีขนาดเท่ากับ 3 ในการทดสอบต่อไปนี้จะทำการทดสอบกับรหัสแอลดีพีซีที่กำหนดให้ “1” ในแต่ละหลักในเมทริกซ์มีขนาดมากกว่า 3 ซึ่งในการทดสอบนี้จะเปรียบกับรหัสแอลดีพีซีที่ใช้โครงสร้างของรหัสบีไอบีดีที่ได้กล่าวไว้ในบทที่ 3 แต่เลือกบล็อกที่นำมาต่อกันเพียง 2 บล็อกเพื่อให้ได้อัตรารหัสเท่ากับ 0.5 โดยรหัสบีไอบีดีมีการออกแบบ 2 แบบ คือ รหัสบีไอบีดีคลาส I และ รหัสบีไอบีดีคลาส II โดยทั้ง 2 แบบกำหนดกำหนดให้น้ำหนัก 1 ในแนวตั้งเมทริกซ์เท่ากับ 4 และ 5 ตามลำดับ โดยพารามิเตอร์ในการ

ออกแบบในการทดสอบนี้ดังตารางที่ 4.8 ทั้งนี้ขนาดเมทริกซ์ตรวจสอบพาริตี้ที่นำมาทดสอบจะออกแบบให้มีขนาดที่ใกล้เคียงกันมากที่สุดเนื่องจากไม่สามารถที่จะออกแบบให้เท่ากันได้ด้วยเงื่อนไขวิธีการออกแบบของโครงสร้างบีไอบีดี และในส่วนของผลการทดสอบสมรรถนะของรหัสแอลดีพีซีดังรูปที่ 4.8

ตารางที่ 4.8 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.5

Type	Code	m	n	j	k	t	p	Girth	Iteration
BIBD I	0.5	313	626	4	8	26	-	6	20
BIBD II	0.5	281	562	5	10	14	-	6	20
QC Proposed	0.5	321	642	3	6	-	107	8	20



รูปที่ 4.8 สมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.5

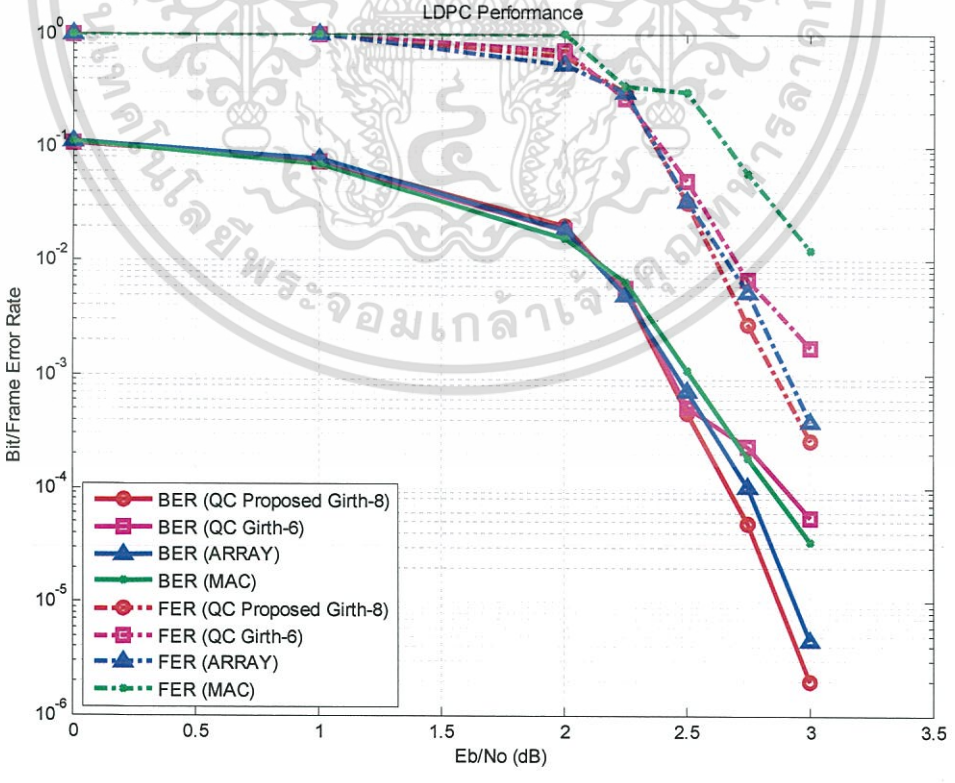
จากผลการทดสอบในรูปที่ 4.8 รหัสแอลดีพีซีที่ออกแบบด้วยโครงสร้างบีไอบีดีคลาส II ให้สมรรถนะที่ดีกว่าแบบคลาส I ทั้งนี้เนื่องจากน้ำหนัก 1 ในแนวตั้งและจำนวน “1” ทั้งหมดในเมทริกซ์มีจำนวนที่มากกว่า แต่เมื่อนำโครงสร้างบีไอบีดีคลาส II เปรียบเทียบกับรหัสแอลดีพีซีบนโครงสร้างควอไซไซคลิคของงานวิจัยนี้ที่มีเกิรธเท่ากับ 8 สมรรถนะที่ได้นั้นด้อยกว่าอยู่ประมาณ

1.25 dB ในส่วนของอัตราบิตผิดพลาด และห่างกันมากกว่า 1.25 dB ในส่วนของอัตราเฟรมผิดพลาด ซึ่งเป็นข้อพิสูจน์ว่ารหัสแอลดีพีซีที่ออกแบบของงานวิจัยนี้แม้ว่าน้ำหนัก 1 ในแนวตั้งมีจำนวนน้อยกว่ารหัสบีไอบีดีแต่เมทริกซ์ที่มีเกิรธมากกว่าส่งผลต่อสมรรถนะในการแก้ไขข้อมูลผิดพลาด และทำให้รหัสที่ออกแบบในวิจัยนี้ดีกว่ารหัสแอลดีพีซีที่ออกแบบด้วยโครงสร้างบีไอบีดีทั้ง 2 แบบ

การทดสอบต่อไปจะทดสอบรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.7 และทำการทดสอบเปรียบเทียบกับรหัสแอลดีพีซีที่ออกแบบบนโครงสร้างรหัสควอไซไซคลิค, รหัสอาร์เรย์ และรหัสอาร์เรย์แบบปรับปรุง โดยพารามิเตอร์ในการทดสอบนี้ดังตารางที่ 4.9 และผลทดสอบสมรรถนะดังรูปที่ 4.9

ตารางที่ 4.9 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.7

Type	Code	m	n	j	k	p	Girth	Iteration
ARRAY	0.7	933	3,110	3	10	311	6	20
MAC	0.7	933	3,110	3	10	311	6	20
QC	0.7	933	3,110	3	10	311	6	20
QC Proposed	0.7	933	3,110	3	10	311	8	20



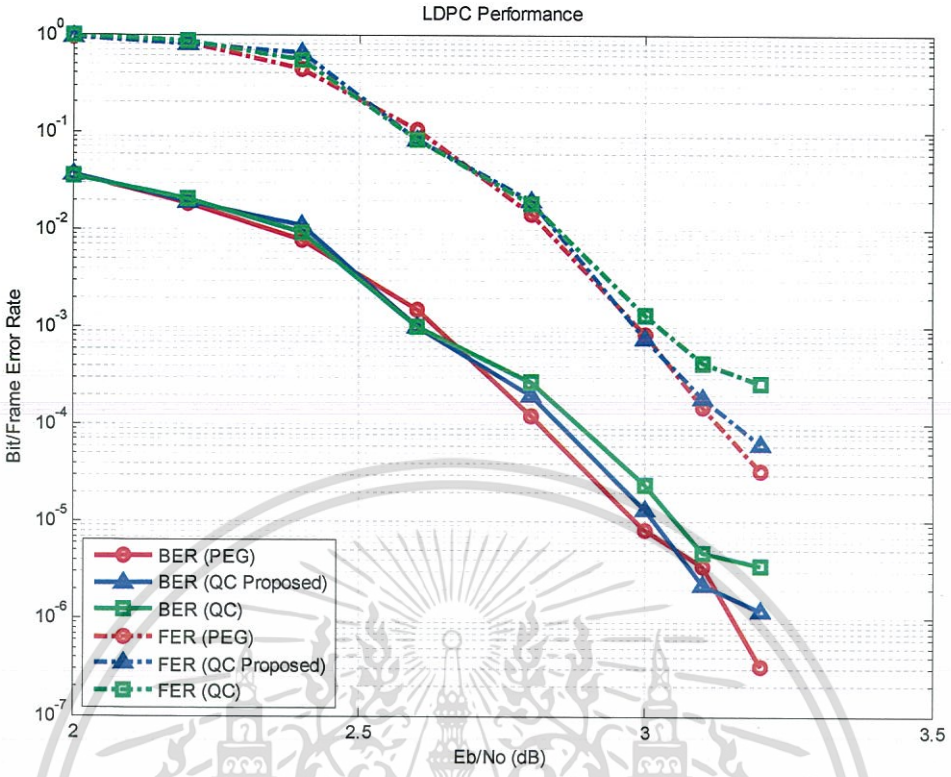
รูปที่ 4.9 สมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.7

จากผลการทดสอบในรูปที่ 4.9 แสดงให้เห็นสมรรถนะของรหัสแอลดีพีซีงานงานวิจัยนี้ที่มีการแก้ไขข้อมูลผิดพลาดได้ดีกว่ารหัสอาร์เรย์ไม่มากนักที่อัตรารหัสสูง แต่สมรรถนะของรหัสแอลดีพีซีที่นำเสนอในงานวิจัยนี้มีสมรรถนะที่ดีกว่ารหัสอาร์เรย์แบบปรับปรุงและรหัสควอไซไซคลิคอย่างมาก แต่ทั้งนี้รหัสแอลดีพีซีที่นำมาเปรียบเทียบเป็นการออกแบบใช้การสุ่มค่าเพื่อกำหนดค่าเมทริกซ์หมุนสลับตำแหน่งซึ่งอาจจะไม่ใช่เมทริกซ์ตรวจสอบพาริตี้ที่ดีที่สุด แต่การทดสอบนี้ยังคงแสดงให้เห็นถึงประสิทธิภาพของการออกแบบเมทริกซ์ที่มีเกิรธ 8 ยังคงมีสมรรถนะที่ดีกว่าเกิรธ 6

ในการทดสอบต่อไปนี้จะกำหนดค่าอัตรารหัสที่ 0.75 โดยจะเปรียบเทียบรหัสแอลดีพีซีของงานวิจัยนี้เปรียบเทียบกับรหัสแอลดีพีซีที่ใช้อัลกอริทึมพีอีจีและรหัสควอไซไซคลิคที่ออกแบบด้วยวิธีการของ Tanner [13] เพื่อทดสอบสมรรถนะที่อัตรารหัสสูง โดยรหัสที่ออกแบบในการทดสอบนี้จะไม่มีรหัสใดเลยที่สามารถสร้างโกลบอลเกิรธได้เท่ากับ 8 แต่ทั้งนี้รหัสแอลดีพีซีของวิจัยนี้และรหัสแอลดีพีซีที่ใช้อัลกอริทึมพีอีจีจะมีโลคอลเกิรธเท่ากับ 6 และ 8 ดังพารามิเตอร์ในการออกแบบดังตารางที่ 4.10 และผลเปรียบเทียบสมรรถนะของรหัสแอลดีพีซีดังรูปที่ 4.10

ตารางที่ 4.10 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.75

Type	Code	m	n	j	k	p	Girth	Iteration
PEG	0.75	303	1,515	3	14,15,16	-	6=809 8=706	20
QC Proposed	0.75	303	1,515	3	15	101	6=1,414 8=101	20
QC	0.75	303	1,515	3	15	101	6=1,515 8=0	20



รูปที่ 4.10 สมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.75

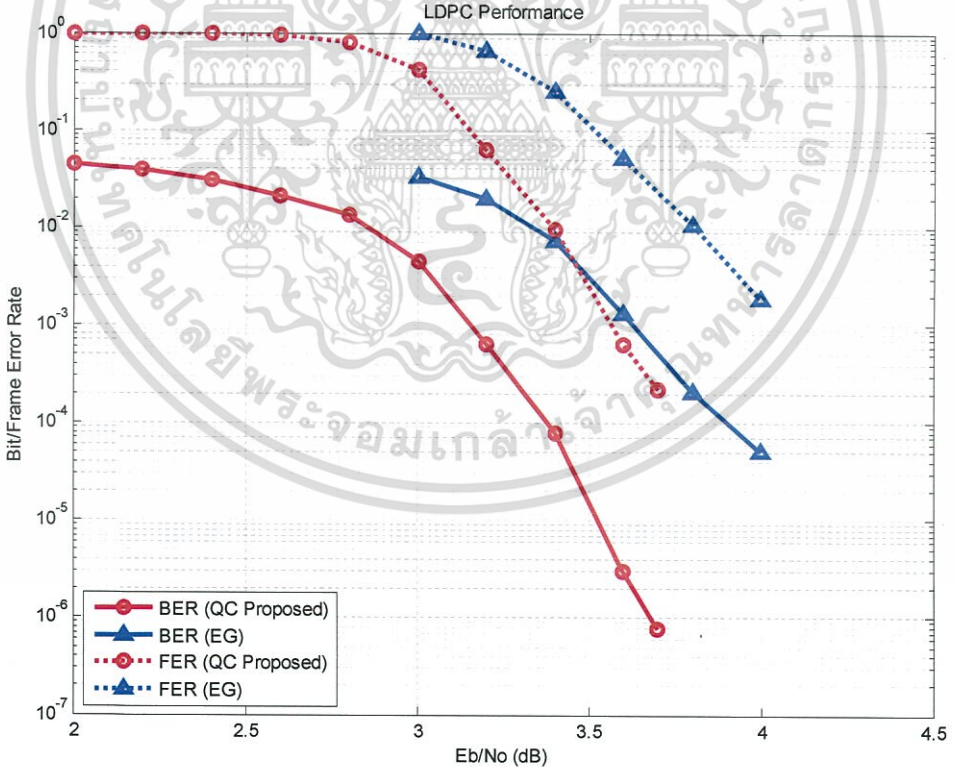
จากรูปที่ 4.10 ผลการเปรียบเทียบสมรรถนะของรหัสแอลดีพีซีที่อัตรารหัส 0.75 จากผลที่ได้รหัสแอลดีพีซีที่ออกแบบด้วยอัลกอริทึมพีอีจีมีสมรรถนะที่ดีกว่ารหัสแอลดีพีซีของวิจัยนี้ แต่รหัสแอลดีพีซีของวิจัยนี้ยังคงมีสมรรถนะดีกว่ารหัสแอลดีพี [13] ถึงแม้ว่ารหัสแอลดีพีซีทั้ง 3 แบบมีโกลบอลเกิรธที่เท่ากันคือ 6 แต่เมื่อพิจารณาถึงจำนวนโลคอลเกิรธแล้ว รหัสแอลดีพีซีโดยใช้อัลกอริทึมพีอีจีมีจำนวนโลคอลเกิรธเท่ากับ 8 มากที่สุดและรหัสแอลดีพีซีของงานวิจัยนี้มีจำนวนโลคอลเกิรธน้อยลงมาและรหัสแอลดีพีซี [13] ไม่มีโลคอลเกิรธเท่ากับ 8 เลย ซึ่งแสดงให้เห็นถึงจำนวนของโลคอลเกิรธสามารถชี้วัดสมรรถนะของรหัสแอลดีพีซีได้เช่นกัน ดังนั้นในการออกแบบแอลดีพีซีที่อัตรารหัสสูงบางครั้งการออกแบบเมทริกซ์ตรวจสอบพาริตี้เป็นไปได้ยากที่จะออกแบบให้ได้โกลบอลเกิรธที่ต้องการ ดังนั้นจึงจำเป็นที่จะต้องพิจารณาโลคอลเกิรธควบคู่กันด้วยเพื่อให้ได้รหัสแอลดีพีซีที่มีสมรรถนะที่ดีที่สุด

การทดสอบต่อไปจะเป็นการทดสอบรหัสแอลดีพีซีที่อัตรารหัส 0.82 โดยเปรียบเทียบกับรหัสแอลดีพีซีที่ออกแบบด้วยเรขาคณิตขอบเขตจำกัดซึ่งมีการออกแบบแบ่งย่อยอีก 2 แบบ คือ รหัสคณิตยูคลิดและรหัสเรขาคณิตเชิงภาพฉายซึ่งมีพารามิเตอร์ที่ใกล้เคียงโดยทั้ง 2 แบบเป็นรหัสแอลดีพีซีที่มีขนาดเกิรธเท่ากับ 6 แต่มีระยะห่างต่ำสุดค่อนข้างสูงมาก โดยในการทดสอบจะเลือกรหัสเรขาคณิตยูคลิดเนื่องจากการออกแบบที่อัตรารหัสสูงจะทำการคำนวณบนคณิตศาสตร์กาลัวส์ที่เลขยกกำลังหรือออร์เดอร์ของพหุนามที่ต่ำกว่าและง่ายต่อการออกแบบ รวมทั้งเป็นรหัสแอลดีพีซีที่

องค์การบริหารการบินและอวกาศแห่งชาติ (National Aeronautics and Space Administration - NASA) ให้ความสนใจ [28] ด้วยระยะห่างต่ำสุดของรหัสเรขาคณิตยูคลิดมี Error floor ของอัตราบิตผิดพลาดน้อยกว่า 10^{-10} ส่วนรหัสแอลดีพีซีของงานวิจัยนี้เนื่องขนาดของข้อมูลอินพุทและอัตรารหัสไม่สามารถที่จะออกแบบให้มีโลคอลเกิรธเท่ากับ 8 ได้จึงเลือกการออกแบบที่สร้างเกิรธได้เท่ากับ 6 มาทดสอบ พารามิเตอร์ของการออกแบบในการทดสอบนี้ดังตารางที่ 4.11 และผลการทดสอบสมรรถนะดังรูปที่ 4.11

ตารางที่ 4.11 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.82

Type	Code rate	m	n	j	k	p	Girth	Iteration
EG	0.82	4,095	4,095	64	64	-	6	20
QC Proposed	0.82	723	4,097	3	17	241	6	20



รูปที่ 4.11 สมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.82

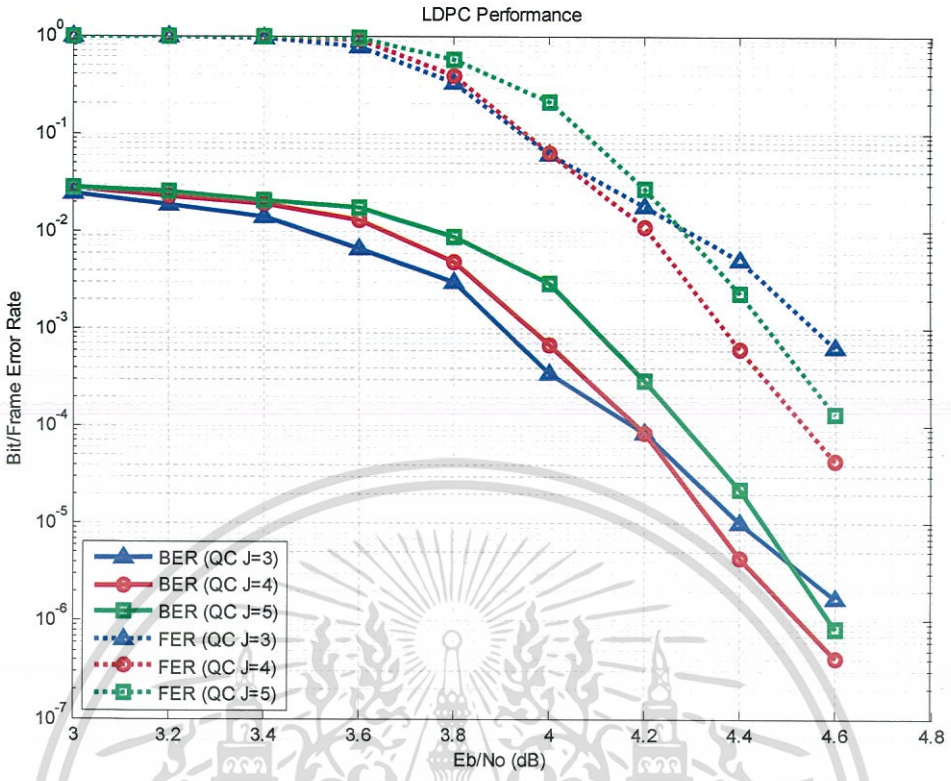
จากรูปที่ 4.11 เมื่อพิจารณาผลการทดสอบสมรรถนะในช่วง 2–4 dB รหัสแอลดีพีซีของงานวิจัยนี้มีสมรรถนะของในส่วนของอัตราบิตผิดพลาดที่ 10^{-7} ที่ Eb/No เท่ากับ 3.5 dB ในขณะที่

รหัสเรขาคณิตยูคลิดอัตราบิตผิดพลาดที่ 10^{-4} เท่านั้น ในการทดสอบนี้ไม่ได้พิสูจน์ได้ว่ารหัสที่ออกแบบในงานวิจัยนี้ดีกว่ารหัสยูคลิดไปทั้งหมด ทั้งนี้หากพิจารณาถึง Error floor แล้ว รหัสเรขายูคลิดน่าจะมีสมรรถนะที่ดีกว่าเนื่องจากระยะห่างต่ำสุดสูงถึง 64 ในขณะรหัสแอลดีพีซีของงานวิจัยนี้ซึ่งเป็นโครงสร้างควอไซไซคลิคและกำหนด “1” ในแนวตั้งเท่ากับ 3 จะมีระยะห่างต่ำสุดได้ไม่เกิน 24 แต่ผลการทดสอบนี้ไม่สามารถที่จะจำลองการทำงานเพื่อหา Error floor ได้เนื่องจากติดข้อจำกัดของเครื่องคอมพิวเตอร์ในการคำนวณและใช้เวลามากในการทดสอบ ดังนั้นการทดสอบนี้จึงต้องการชี้ให้เห็นถึงสมรรถนะในช่วง Eb/No ที่มีค่าต่ำรหัสแอลดีพีซีของวิจัยนี้ว่ามีสมรรถนะดีกว่ารหัสเรขาคณิตยูคลิดในช่วง Eb/No มีค่าต่ำเท่านั้น

ในการทดสอบต่อไปนี้จะทำการทดสอบสมรรถนะของรหัสแอลดีพีซีที่อัตราประมาณ 0.9 โดยที่อัตรารหัสดังกล่าวการออกแบบที่ได้นำเสนอจะไม่สามารถสร้างเกิรธได้เกิน 6 ดังนั้นจะทดสอบโดยการปรับเปลี่ยนค่า “1” ในหลักของเมทริกซ์ตรวจสอบพาริตี้ดังตารางที่ 4.12 และผลการทดสอบสมรรถนะดังรูปที่ 4.12

ตารางที่ 4.12 พารามิเตอร์ในการสร้างรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.9

Type	Code rate	m	n	j	k	p	Girth	Iteration
QC	0.9	411	4,110	3	30	137	6	20
QC	0.9	412	4,120	4	40	103	6	20
QC	0.9	415	4,150	5	50	83	6	20



รูปที่ 4.12 สมรรถนะของรหัสแอลดีพีซีที่อัตรารหัสเท่ากับ 0.9

จากผลการทดสอบสมรรถนะในรูปที่ 4.12 สำหรับรหัสแอลดีพีซีที่ใช้อัตรารหัสสูงที่ประมาณ 0.9 ผลที่ได้แสดงให้เห็นถึงการเพิ่มน้ำหนัก 1 ในแนวตั้งของเมทริกซ์ตรวจสอบพาริตี้ส่งผลให้สมรรถนะโดยรวมของรหัสแอลดีพีซีดีขึ้น โดยรหัสแอลดีพีซีที่กำหนดให้น้ำหนัก 1 ในแนวตั้ง $j=4$ จะมีสมรรถนะที่ดีกว่า น้ำหนัก 1 ในแนวตั้ง $j=3$ และ $j=5$ แต่หากพิจารณาความชันของกราฟที่ได้ รหัสแอลดีพีซีที่กำหนดให้ น้ำหนัก 1 ในแนวตั้ง $j=5$ มีความชันของกราฟมากที่สุดและหากพิจารณาสมการที่ (3.5) ในบทที่ 3 การออกแบบรหัสแอลดีพีซีให้ได้ระยะห่างต่ำสุดให้มีค่ามากขึ้นอยู่กับเกิรธและน้ำหนัก 1 ในแนวตั้งในเมทริกซ์ตรวจสอบพาริตี้ รหัสแอลดีพีซีที่กำหนดให้น้ำหนัก 1 ในแนวตั้ง $j=5$ หากเกิรธเท่ากันจะมีระยะห่างต่ำสุดที่มากกว่าน้ำหนัก 1 ในแนวตั้ง $j=3$ และ $j=4$ ดังนั้นในการออกแบบรหัสแอลดีพีซีด้วยวิธีการที่เสนอในงานวิจัยนี้ในส่วนอัตราที่สูงมากและไม่สามารถสร้างเกิรธมากกว่า 6 ได้ การออกแบบโดยการกำหนดให้น้ำหนัก 1 ในแนวตั้ง j ที่มากขึ้นจึงเป็นอีกวิธีหนึ่งในการออกแบบเพื่อให้ได้เมทริกซ์ตรวจสอบที่สมรรถนะที่ดี แต่ทั้งนี้การเพิ่มน้ำหนัก 1 ในแนวตั้ง j มากขึ้นทำให้ “1” ในเมทริกซ์ตรวจสอบพาริตี้มีจำนวนที่มากตาม ซึ่งอาจไม่เหมาะสมในการนำไปประยุกต์ใช้สร้างฮาร์ดแวร์เนื่องจากจำนวนฮาร์ดแวร์ที่ใช้ที่ต้องเพิ่มวงจรในการถอดรหัสตามจำนวนน้ำหนัก 1 ในแนวตั้งของเมทริกซ์ตรวจสอบพาริตี้ การเลือกกำหนดค่าน้ำหนัก 1 ในแนวตั้ง j จึงต้องเลือกให้เหมาะสมกับการนำไปประยุกต์ใช้งาน

ในบทนี้แสดงวิธีการออกแบบรหัสแอลดีพีซีบนโครงสร้างรหัสควอไซไซคลิคที่สามารถสร้างให้มีขนาดของเกิรธตั้งแต่ 6 ขึ้นไปด้วยการกำหนดเมทริกซ์หมุนสลับตำแหน่งเป็นเลขจำนวนเฉพาะและเลือกอิเลเม้นต์ที่เป็นเลขจำนวนเฉพาะที่เมื่อยกกำลังเพิ่มขึ้นและมอดูโลด้วยค่าขนาดของเมทริกซ์หมุนสลับตำแหน่งแล้วมีเซตร่วมครบทุกค่าเพื่อออกแบบรหัสแอลดีพีซีที่ขนาดเกิรธเท่ากับ 6 และจากเมทริกซ์ตรวจสอบพาริตี้ที่ได้นี้สามารถออกแบบเพื่อเพิ่มขนาดของเกิรธได้ด้วยการเลือกตำแหน่งที่เหมาะสม โดยใช้การนำเมทริกซ์ย่อยในแต่ละหลักมาต่อกัน ทั้งนี้วิธีการออกแบบในงานวิจัยนี้สามารถออกแบบเกิรธขนาด 6, 8, 10 และ 12 ได้ แต่เกิรธที่มีขนาดมากขึ้นต้องให้ขนาดของเมทริกซ์หมุนสลับตำแหน่งที่ใหญ่ตามรวมทั้งเกิรธที่มีขนาดใหญ่เกินเกิรธ 8 จะได้อัตรารหัสที่ลดลง จากนั้นได้ทดสอบเปรียบเทียบสมรรถนะกับรหัสแอลดีพีซีแบบอื่นในแต่ละอัตรารหัส ซึ่งแสดงถึงสมรรถนะของรหัสแอลดีพีซีที่นำเสนอมีสมรรถนะที่ดีกว่ารหัสแอลดีพีซีแบบอื่นๆอยู่หลายแบบ แต่ทั้งนี้ผู้วิจัยจะได้สรุปผลทั้งหมดอีกครั้งอย่างละเอียดในบทถัดไป

บทที่ 5
สรุปผลการวิจัยและข้อเสนอแนะ

5.1 สรุปผลงานวิจัย

จากวัตถุประสงค์ของงานวิจัยนี้ที่ต้องการการออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซีที่ต้องการโครงสร้างแบบแน่นอน ง่ายต่อการออกแบบ มีสมรรถนะที่ดีเมื่อนำไปใช้กับอัตรารหัสค่าต่าง ๆ และเหมาะสมต่อการประยุกต์ใช้งานจริง จากวิธีการออกแบบที่ผู้วิจัยได้นำเสนอเมื่อเปรียบเทียบกับวิธีการออกแบบอื่น สามารถสรุปได้ดังนี้

- รหัสแอลดีพีซีที่ออกแบบบนโครงสร้างรหัสควอไซไซคลิคซึ่งเป็นรหัสที่มีวงจรในการเข้ารหัสเร็วโดยใช้วงจรเข้ารหัส Cyclic shift register-adder-accumulator ที่ได้กล่าวไว้ในบทที่ 2 โดยความซับซ้อนในการเข้ารหัสของรหัสควอไซไซคลิคจะเพิ่มขึ้นตามจำนวนบิตพาริตี้ ในส่วนการถอดรหัสใช้หน่วยความจำน้อยในเก็บค่าเมทริกซ์ตรวจสอบพาริตี้ หากเปรียบเทียบกับรหัสอาเรย์หรืออัลกอริทึมพีอีจีนั้นจะต้องทำการเข้ารหัสโดยตรงตามสมการการเข้ารหัสโดยใช้วงจรคูณและวงจรบวกในการสร้างวงจรสำหรับการเข้ารหัสและไม่มีการเข้ารหัสเร็วสำหรับรหัสอาร์เรย์แบบปรับปรุงสามารถออกแบบวงจรในส่วนเข้ารหัสได้เร็วตามวิธีการของ Richardson [23] และความเร็วในการเข้ารหัสจะมีความซับซ้อนเพิ่มมากขึ้นตามขนาดของบล็อกในลักษณะเชิงเส้น
- ส่วนรหัสที่ออกแบบด้วยคณิตศาสตร์ขอบเขตจำกัด เช่น รหัสยูคลิด, รหัสเรขาคณิตเชิงภาพฉาย หรือ รหัสบล็อกไม่สมบูรณ์แบบสมดุล อยู่บนโครงสร้างของรหัสไซคลิกสามารถเข้ารหัสเร็วด้วยวงจรเข้ารหัสไซคลิกและใช้หน่วยความจำน้อยสำหรับการเก็บข้อมูลของเมทริกซ์ตรวจสอบพาริตี้
- เมื่อพิจารณาต่อถึงความง่ายในการออกแบบรหัสแอลดีพีซีที่นำเสนอวิจัยนี้หากเปรียบเทียบกับกับรหัสที่ออกแบบด้วยคณิตศาสตร์ขอบเขตจำกัดซึ่งใช้คณิตศาสตร์ที่เข้าใจยากต่อผู้เริ่มต้นเนื่องจากจะต้องเข้าใจกาลัวส์ฟิลด์จึงจะสามารถออกแบบรหัสแอลดีพีซีบนโครงสร้างดังกล่าวได้ ในส่วนรหัสที่นำเสนอในงานวิจัยนี้ใช้เพียงคณิตศาสตร์พื้นฐานคือลำดับเรขาคณิตและกลุ่มผลคูณของการมอดูโลเลขจำนวนเต็ม p ซึ่งง่ายต่อความเข้าใจสำหรับผู้เริ่มต้น
- เปรียบเทียบกับรหัสควอไซไซคลิคที่มีรูปแบบคล้ายกัน เช่น รหัสแอลดีพีซีที่เสนอโดย Tanner [13] หรือการรหัสแอลดีพีซีที่ใช้ Cycotomic coset [14] ทั้งสองวิธีเมื่อกำหนดค่าเมทริกซ์ย่อยในแถวแรกได้แล้วต้องคำนวณหาค่าเมทริกซ์หมุนสลับตำแหน่งในแถวถัดไปจนครบ แต่วิธีการออกแบบของงานวิจัยนี้จะคำนวณหาค่าในแถวแรกเท่านั้น ส่วนแถวถัดไปใช้การเลื่อนเมทริกซ์ย่อยในแถวแรกทีละครั้งโดยไม่ต้องทำการคำนวณหาค่าเมทริกซ์ย่อยในแต่ละแถว
- ในส่วนของการออกแบบเพื่อสร้างเมทริกซ์ให้มีขนาดของเกิรธเท่ากับหรือมากกว่า 8 ในการค้นหาลำดับหรือตำแหน่งของหลักหากเปรียบเทียบกับงานวิจัย [16] นั้นอาจใกล้เคียงกัน แต่ในส่วนของรหัสแอลดีพีซีในงานวิจัยนี้สามารถลดขั้นตอนได้โดยการตัดหลักใดหลักหลักหนึ่ง

ในบล็อกย่อยขนาด 3×3 ซึ่งเป็นหลักที่ทำให้เกิดเกิรธ 6 จึงไม่จำเป็นที่จะต้องตรวจสอบทุกหลัก

- ในส่วนของสมรรถนะของรหัสแอลดีพีซีนั้นผู้วิจัยมุ่งเน้นไปที่การสร้างให้เกิรธที่มีขนาดมากกว่า 6 ซึ่งเกิรธที่ใหญ่ขึ้นจะส่งผลต่อสมรรถนะโดยรวม จากผลการทดสอบสมรรถนะในบทที่ 4 รหัสแอลดีพีซีที่นำเสนอในงานวิจัยนี้ที่มีเกิรธเท่ากับ 8 มีสมรรถนะที่ดีกว่ารหัสแอลดีพีซีอื่นๆที่ออกแบบและได้เกิรธเท่ากับ 6 หลายวิธีและหลายอัตรารหัส
- ในการเปรียบเทียบกับรหัสแอลดีพีซีที่ออกแบบและเกิรธขนาดที่เท่ากันคือ เกิรธเท่ากับ 8 ด้วยวิธีการออกแบบของ [16] ซึ่งมีวิธีการย่อยออกเป็น 3 แบบ คือ MWC, QCS แลพ SP ผลที่ได้คือรหัสแอลดีพีซีในงานวิจัยนี้มีประสิทธิภาพที่เทียบเท่าวิธีการ MWC และมีสมรรถนะที่ดีวิธีการ QCS และ SP เนื่องจากมีระยะห่างต่ำสุดมีค่ามากกว่า
- ในส่วนของการเปรียบเทียบกับรหัสแอลดีพีซีที่สามารถสร้างเกิรธขนาดใหญ่อย่างอัลกอริทึมพีอีจี หากเกิรธของอัลกอริทึมพีอีจีมีได้ขนาดเกิรธที่ได้เท่ากันสมรรถนะของรหัสแอลดีพีซีที่นำเสนอในงานวิจัยนี้จะด้อยกว่าเล็กน้อย แต่ทั้งนี้หากพิจารณาส่วนวงจรถอดรหัสในการจัดเก็บเมทริกซ์ตรวจสอบพาริตี้และการคำนวณการถอดรหัส อัลกอริทึมพีอีจีต้องใช้หน่วยความจำที่มากกว่าและวงจรคำนวณในการถอดรหัสก็มีความซับซ้อนมากกว่าโครงสร้างรหัสควอไซไซคลิคอันเนื่องมาจากโครงสร้างอัลกอริทึมพีอีจีเป็นโครงสร้างแบบสุ่ม
- การออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซีเพื่อให้ได้สมรรถนะที่ดีนั้นควรออกแบบให้เมทริกซ์ปราศจากลูป 4 และมีเกิรธที่มีขนาดใหญ่มากที่สุดเท่าที่จะมากได้ เนื่องจากเกิรธจะส่งผลต่อการลู่เข้าหาข้อมูลที่ถูกต้องในการถอดรหัส
- การออกแบบที่เสนอในงานวิจัยนี้เพื่อให้ได้เกิรธที่ใหญ่ต้องกำหนดให้ขนาดของเมทริกซ์หมุนสลับตำแหน่งต้องมีขนาดที่ใหญ่ตามและเกิรธที่ใหญ่มากเช่น เกิรธ 10 หรือ 12 ไม่สามารถที่จะออกแบบสำหรับอัตรารหัสสูงมากได้
- นอกเหนือจากเกิรธแล้วน้ำหนัก 1 ในแนวตั้งของเมทริกซ์เป็นตัวแปรที่สำคัญอีกอย่างหนึ่ง เนื่องจากน้ำหนัก 1 ในแนวตั้งของเมทริกซ์ที่เพิ่มขึ้นจะทำให้ระยะห่างต่ำสุดมีค่าที่มากขึ้นด้วยและส่งผลให้ Error floor ของอัตราบิตผิดพลาดและอัตราเฟรมผิดพลาดมีค่าต่ำหรือกล่าวคือรหัสแอลดีพีซีมีความสามารถในการแก้ไขข้อมูลหรือบิตผิดพลาดได้ดียิ่งขึ้น แต่การเพิ่มน้ำหนัก 1 ในแนวตั้งที่มากขึ้นจะทำให้มี “1” ในเมทริกซ์ตรวจสอบพาริตี้มากตามทำให้ยากต่อการสร้างเมทริกซ์เพื่อให้ได้เกิรธที่มีขนาดใหญ่และทำให้การสร้างเป็นฮาร์ดแวร์มีความซับซ้อนและขนาดที่ใหญ่ตามด้วย
- การหาระยะห่างต่ำสุดไม่สามารถจะคำนวณหาค่าได้โดยตรง วิธีการหนึ่งที่จะหาค่าประมาณระยะห่างต่ำสุดคือการทดสอบด้วยจำลองการทำงานด้วยโปรแกรมหาค่าโดยประมาณของระยะห่างต่ำสุด [27] ดังนั้นการเลือกโครงสร้างในการออกแบบรหัสแอลดีพีซีหากต้องการนำไปประยุกต์ใช้งานจริงหรือนำไปสร้างเป็นฮาร์ดแวร์ควรเลือกโครงสร้างของรหัสแอลดีพีซีที่มีวงจรที่ง่ายรองรับการออกแบบเพื่อลดความยุ่งยากในการสร้างฮาร์ดแวร์ ทั้งนี้โครงสร้างที่กล่าวมานี้อาจจะไม่ใช่โครงสร้างที่ทำให้แอลดีพีซีมีสมรรถนะดีที่สุด ดังนั้นในการใช้งานจึงต้องเลือกให้เหมาะสมกับงานนั้นๆ

จากการสรุปทั้งหมดการออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซีในงานวิจัยนี้จึงเป็นไปตามวัตถุประสงค์ตั้งไว้และเป็นการออกแบบที่สามารถนำไปประยุกต์ใช้ในระบบสื่อสารหรือระบบบันทึกข้อมูลได้

5.2 ข้อเสนอแนะ

การออกแบบเมทริกซ์ตรวจสอบพาริตี้ของรหัสแอลดีพีซีในงานวิจัยนี้เป็นรหัสแก้ไขข้อผิดพลาดด้วยรหัสบล็อก แต่ทั้งนี้รหัสแอลดีพีซียังสามารถที่จะนำไปใช้ในแบบรหัสคอนโวลูชั่น (Convolution codes) ได้ [13] และจากบทความที่นำเสนอวิธีการดังกล่าวนี้ได้เปรียบเทียบสมรรถนะระหว่างรหัสแอลดีพีซีแบบรหัสบล็อกกับแบบรหัสคอนโวลูชั่น ผลที่ได้คือรหัสคอนโวลูชั่นมีสมรรถนะที่เหนือกว่ารหัสบล็อก จากวิธีการออกแบบในงานวิจัยของวิทยานิพนธ์ฉบับนี้ซึ่งมีพื้นฐานการออกแบบมาจาก [13] ซึ่งน่าจะทำการออกแบบเพื่อใช้ในรหัสคอนโวลูชั่นได้เช่นกันและอาจเป็นวิธีการที่จะพัฒนารหัสแอลดีพีซีให้ประสิทธิภาพที่สูงขึ้นอีกได้ในอนาคต

บรรณานุกรม

[1] C. E. Shannon, "Mathematical Theory of Communication," **Bell System Technical Journal**, vol.27, pp379-423, 623-656, October 1948.

[2] Draft STANDARD for Information Technology – Telecommu-nications and information exchange between systems - Local and metropolitan area networks – Specific requirements-, IEEE P802.11n./D3.00, Sptember 2007.

[3] IEEE Standard for Local and metropolitan area networks Part 16: Air Interface for Broadband Wireless Access Systems, IEEE Std 802.16-2009, pp. C1-2004, 2009.

[4] R. Gallager, "Low-density parity-check codes," **IRE Trans. Inform. Theory**, vol. 8, pp. 21-28, 1962.

[5] R. Tanner, "A recursive approach to low complexity codes," **IEEE Trans. Inform. Theory**, vol. 27, pp. 533-547, 1981.

[6] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes," **Proc. IEEE Int. Conf. Commun. (ICC)**, vol.2, pp. 1064-1070, May 1993.

[7] D. J. C. MacKay and R. M. Neal, "Near Shannon limit performance of low density parity check codes," **Electronics Letters**, vol. 32, p. 1645, 1996.

[8] T. J. Richardson, M. A. Shokrollahi, R. L. Urbanke, "Design of capacity-Approaching irregular low-density parity-check codes," **IEEE Trans. Inform. Theory**, Vol. 47, pp. 619-637, Febuary 2001.

[9] S. J. Johnson, Iterative Error Correction Turbo, Low- Density Parity-Check and Repeat-Accumulate Codes. Cambridge University Press, Cambridge 2010.

[10] J. L. Fan, "Array codes as low-density parity check codes," **Proc. 2nd International Symposium on Turbo Codes & Related Topics**, pp. 543-546, 2000.

[11] E. Eleftheriou and S. Olcer, "Low-density parity-check codes for digital subscriber lines," **Proc. IEEE Int. Conf. Commun. (ICC)**, vol.3 pp. 1752-1757, 2002.

[12] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," **IEEE Trans. Inform. Theory**, vol. 50, no.8, pp. 1788–1793, August 2004.

[13] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello, Jr., "LDPC block and convolutional codes based on circulant matrices," **IEEE Trans. Inform. Theory**, vol. 50, no. 12, pp. 2966–2984, December 2004.

[14] M. Esmaeili, M. Najafian, and A. T. Gulliver, "Structured quasi-cyclic low-density parity-check codes based on cyclotomic cosets," **IET Communications**, vol. 9, pp. 541-547, 2015.

[15] C. M. Huang, J. F. Huang, and C. C. Yang, "Construction of quasicyclic LDPC codes from quadratic congruences," **IEEE Commun. Lett.**, vol. 12, no. 4, pp. 313–315, April 2008.

[16] J. F. Huang, C. M. Huang, and C. C. Yang, "Construction of onecoincidence sequence quasi-cyclic LDPC codes of large girth", **IEEE Trans. Inform. Theory,** vol. 58, no. 3, pp. 1825–1836, March 2012.

[17] Y. Kou, S. Lin, and M. Fossorier, "Low density parity check codes based on finite geometries: a rediscovery," **Proc. IEEE Int. Symp. Information Theory**, Sorrento, p. 200, June 2000.

[18] Y. Kou, S. Lin, and M. Fossorier, "Construction of low density parity check codes: a geometric approach," Proc. 2nd Int. Symp. **Turbo Codes and Related Topics,** Brest, pp. 137–140, September 2000.

[19] Y. Kou, S. Lin, and M. Fossorier, "Low-density parity-check codes based on finite geometries: a rediscovery and new results," **IEEE Trans. Inform. Theory**, vol. 47, no. 7, pp. 2711–2736, November 2001.

[20] B. Ammar, B. Honary, Y. Kou, J. Xu, and S. Lin, "Construction of low density parity-check codes based on balanced imcomplete block designs," **IEEE Trans. Inform. Theory**, vol. 50, no. 6, pp. 1257-1268, June 2004.

[21] L. Lan, Y. Y. Tai, S. Lin, B. Memari, and B. Honary, "New construction of quasi-cyclic LDPC codes based on special classes of BIBD's for the AWGN and binary erasure channels," **IEEE Trans. Communications**, vol. 56, no. 1, pp. 39–48, January 2008.

[22] X. Y. Hu, E. Eleftheriou, and D. M. Arnold, "Progressive Edge-Growth Tanner Graphs," **Proc. IEEE Global Telecomm. Conf. (GLOBECOM)**, pp. 995-1001, November 2001.

[23] T. J. Richardson and R. Urbanke, "Efficient encoding of low-density parity-check codes", **IEEE Trans. Inform. Theory**, vol. 47, no. 2, pp. 638–656, Febuary 2001.

[24] S. Timakul, S. Choomchuay, "A simple algorithm for a high code rate LDPC parity matrix design," **International Symposium on Communications and Information Technologies (ISCIT)**, October 2011.

[25] S. Timakul, S. Choomchuay, "Construction of Quasi-Cyclic LDPC Codes form SFT Structure and Cyclic Shift," **Intelligent Signal Processing and Communications Systems (ISPACS)**, December 2011.

[26] S. Timakul, S. Choomchuay, "A simple parity check matrix LDPC code for perpendicular magnetic recording channels," **Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)**, May 2013.

[27] D. MacKay, Gallager code esources [Online], Available: http://www.inference.phy.cam.ac.uk/mackay/CodesFiles.html

[28] http://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/20030106684.pdf

[29] S. Timakul, S. Koonkarnkhai, P. Kovintavewat, and S. Choomchuay, "A Concatenate Code for Error Correcting Code in Bit Pattern Media Recoding System," **Advanced Materials Research**, Vols. 834-836 pp 962-967, 2014.

[30] S. Timakul, S. Choomchuay, "A Construction of Non Binary LDPC Codes by Circular Matrices," **Advanced Materials Research**, Vol. 909 pp 338-341, 2014.

ภาคผนวก

ภาคผนวก ก.

ตารางสัญลักษณ์

สัญลักษณ์	ความหมายของสัญลักษณ์
S	เซต (Set)
α	อิลิเมนต์ (Elements)
$\mathbf{m}$	ข้อมูลอินพุทข่าวสาร (Massage)
$\mathbf{c}$	คำรหัส (Codeword)
$\hat{\mathbf{c}}$	คำรหัสที่ผ่านการถอดรหัส
$\mathbf{H}$	เมทริกซ์ตรวจหาพาริตี้ (Parity Check Matrix)
$\mathbf{G}$	เมทริกซ์กำเนิด (Generator Matrix)
$GF(q)$	กาลัวส์ฟิลด์ (Galois Field) ในฟิลด์ q
R	อัตรารหัส (Code Rate)
$\mathbf{I}$	เมทริกซ์เอกลักษณ์ (Identity Matrix)
$\mathbf{P}$	เมทริกซ์หมุนสลับตำแหน่ง (Permutation Matrix)
j	น้ำหนัก 1 ในแนวตั้ง (Column weigth) ของเมทริกซ์ตรวจสอบพาริตี้
k	น้ำหนัก 1 ในแนวนอน (Row weigth) ของเมทริกซ์ตรวจสอบพาริตี้
m	ขนาดของเมทริกซ์ตรวจสอบพาริตี้ในแนวตั้ง
n	ขนาดของเมทริกซ์ตรวจสอบพาริตี้ในแนวนอน
$d_{\min}$	ระยะห่างต่ำสุด (Minimum Distance)
p	ขนาดของเมทริกซ์หมุนสลับตำแหน่ง
λ	สัดส่วนระหว่างผลรวมของจำนวนสมาชิกที่ไม่เป็นศูนย์ของทุกหลักในเมทริกซ์ $\mathbf{H}$
ρ	สัดส่วนระหว่างผลรวมของจำนวนสมาชิกที่ไม่เป็นศูนย์ของทุกแถวในเมทริกซ์ $\mathbf{H}$
w_v	จำนวน “1” ในแนวตั้งของเมทริกซ์ตรวจสอบพาริตี้
w_c	จำนวน “1” ในแนวนอนของเมทริกซ์ตรวจสอบพาริตี้

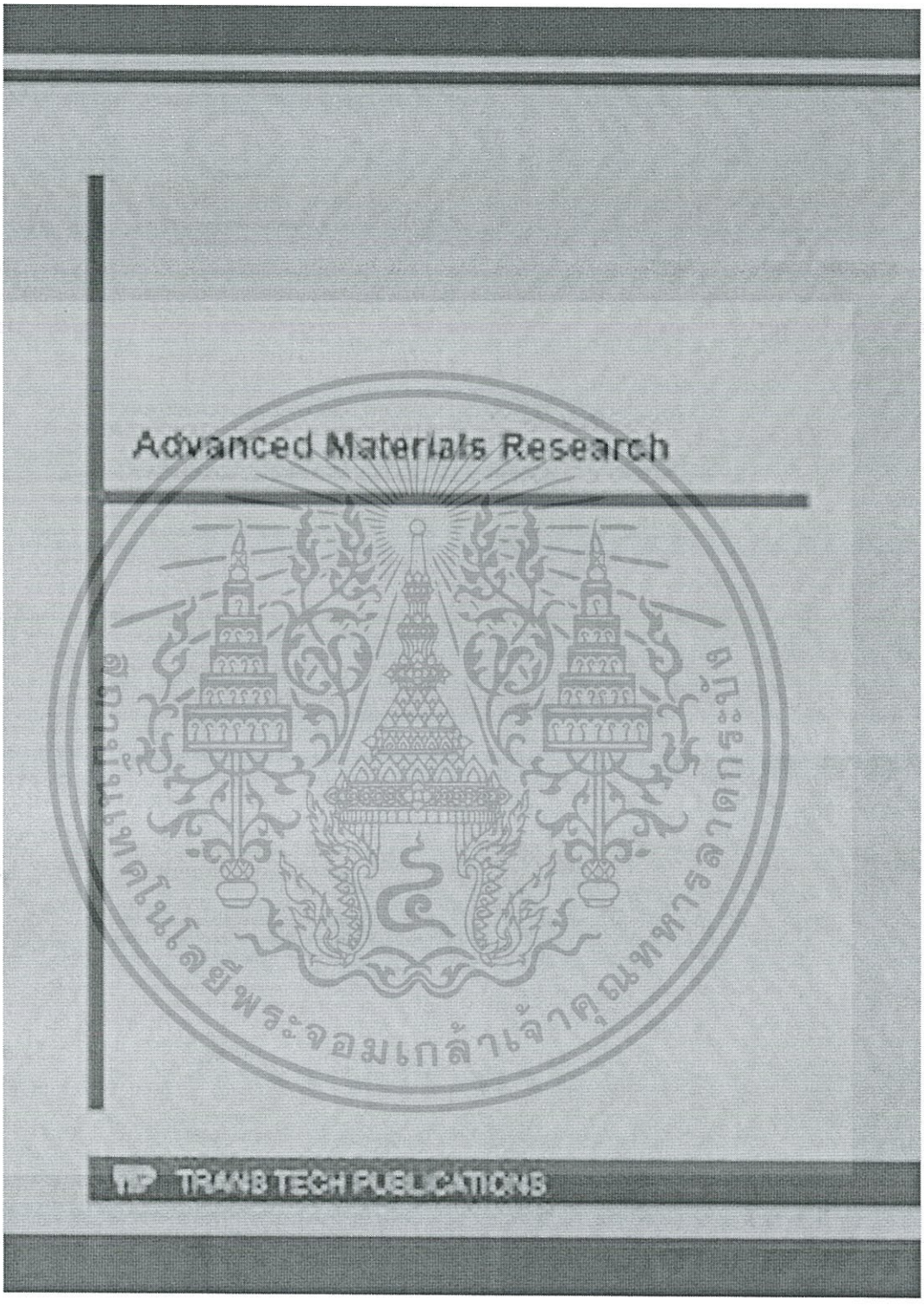
ภาคผนวก ข.
ผลงานวิจัยที่ได้รับการตีพิมพ์เผยแพร่

International Journals

1. S. Timakul, S. Koonkarnkhai, P. Kovintavewat, and S. Choomchuay, "A Concatenate Code for Error Correcting Code in Bit Pattern Media Recoding System," **Advanced Materials Research**, Vols. 834-836 pp 962-967, 2014.
2. S. Timakul, S. Choomchuay, "A Construction of Non Binary LDPC Codes by Circular Matrices," **Advanced Materials Research**, Vol. 909 pp 338-341, 2014.

International Conferences

1. S. Timakul, S. Choomchuay, "A simple algorithm for a high code rate LDPC parity matrix design," **International Symposium on Communications and Information Technologies (ISCIT)**, October 2011.
2. S. Timakul, S. Choomchuay, "Construction of Quasi-Cyclic LDPC Codes form SFT Structure and Cyclic Shift," **Intelligent Signal Processing and Communications Systems (ISPACS)**, December 2011.
3. S. Timakul, S. Choomchuay, "A simple parity check matrix LDPC code for perpendicular magnetic recording channels", **Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)**, May 2013.



Advanced Materials Research Vols. 834-836 (2014) pp 962-967
Online available since 2013/Oct/31 at www.scientific.net

doi:10.4028/www.scientific.net/AMR.834-836.962

A Concatenate Code for Error Correcting Code in Bit Pattern Media Recoding System

S. Timakul[1, a], S. Koonkarnkhai[2], P. Kovintavewat[2], and S. Choomchuay[3, b]

[1]College of Data Storage Innovation, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand, Tel:/Fax: + 66-2-326-4731

[2]Data Storage Technology Research Center, Nakhon Pathom Rajabhat University, Nakhon Pathom, 73000, Thailand

[3]Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand Tel: +66-2-329-8344 Ext.114, Fax: +66-2-329-8346

[a] sekson.timakul@gmail.com, [b] kchsomsa@kmitl.ac.th

Keywords: Magnetics recoding, BPMR, Concatenate code, LDPC, RS code

Abstract Bit Pattern Media Recording (BPMR) is the modern HDD recording technique which can overcome the constraint of conventional technique by offering tremendous areal density. However, narrow track of BPMR can cause noise generating from inter-track interference (ITI) and In. inter-symbol interference (ISI). One traditional technique used to improve BER of the system is the introducing of error control coding. In this paper, we investigate concatenate code applied to BPMR. We proposed inner code with low-density parity-check (LDPC) and Reed-Solomon (RS) codes as outer code. The obtained simulation results confirmed to us that the concatenated coding scheme yielded better performance compared with the single LDPC code deployment.

Introduction

Nowadays, usage of internet and digital communication has growth continuity. This is also one of the major drive for digital storage needs. Hard disk is the most widely used for such the kind of digital storages. A conventional HDD system is composed of recording plate which is coated with a thin film of magnetic (magnetic grain). The size of magnetic grain is in nanometer scale, and each grain is in disordered direction. In order to write data into disk, the recording head needs to control magnetic grain in either perpendicular or longitudinal direction respected to the recording media. An alternative technique to achieve tremendous areal density is to reduce the size of magnetic grain. However, reducing the magnetic grain can cause unstable data in storage and thermal fluctuation. The external heat may effect magnetic characteristic changing. The data bit might change to opposite direction. This phenomenon called super-paramagnetic limit [1].

The new technologies that challenge the conventional one; such as Perpendicular Magnetic Recording (PMR), Heat Assisted Magnetic Recording (HAMR) [2], Bit Patterned Magnetic Recording (BPMR) [3], and Two Dimensional Magnetics Recording (TDMR) [4] are now drawing high interest. Those technologies, the capacity of more than 1 Tb/in^2 can be possible. BPMR is expected to achieve areal density up to 1-4 Tb/in^2 by storing one bit per cell into a single-domain rectangular magnetic island of the nano-meter scale. Researches in recording media have been developed greatly by various techniques such as nanolithography, self-assembly, electron beam lithography and Nano-imprint lithography, etc.

Recently, the areal density at 1 Tb/in^2 has been accomplished via the use of magnetic island. It is already brought to practical applications [5]. BPMR has many advantages such as minimize noise during transition, nonlinear bit shift, ease of data recovery, and facilitate on servo system tracking, etc. Nonetheless, BPMR is still encounter with read channel problem due the reduction of size and shape of the magnetic island. The read back signal may also be influenced by pulse response and the occurrence linear superposition effect between main track and adjacent track called inter-track

interference (ITI). If the distance between island even closer together it may generate inter-symbol interference (ISI) accordingly. Both effects can cause error of data and performance degradation of BPMR during read back process.

Improving BER of the HDD system with the deployment of error control code is commonly known. Reed Solomon code has been used intensively from the very beginning of HDD development to some years after 2000. Since the re-discovery of LDPC code in late 1990, such codes had been applied to HDD system and gradually replace Reed Solomon code. Either Reed Solomon code or LDPC code, only one coding scheme is used and concatenation of codes is not yet found in the published literatures.

In this paper, we propose an error correction coding scheme to correct the error of read back data. We will examine a BPMR channel with areal density of 2 Tb/in^2 and 2.5 Tb/in^2. A single reading head and partial response maximum likelihood (PMRL) is the environment used. At the receiver, 1-D target and 1-D equalizer with decoder soft-input soft-output (SISO) detector are used. Within SISO detector, the soft output viterbi algorithm (SOVA) and SISO decoder with Low Density Parity Check Code (LDPC) are deployed. An extra error correction code, Reed Solomon Code (RS), is added to the system. Basically those 2 coded are concatenated. The performance of the system is measured in term of bit error rate (BER) and sector error rate (SER) versus signal to noise ratio (SNR). The obtained results can clarify to us the benefit of using RS-LDPC concatenated code.

Channel Model

In BPMR, the change of magnetic islands characteristics which are uniformly distributed on the media, is influenced by the 2-D pulse response. Relevent parameters to model the BPMR channel are given by [6] and [7], where the 2-D Gaussian pulse response $H(x,z)$ is written as

$$H(x,z) = A\exp\left\{-\frac{1}{2}\left(\frac{x^2}{w_x^2}+\frac{z^2}{w_z^2}\right)\right\}, \tag{1}$$

The coefficients of a channel, $H(D)$, can be obtained by sampling (1) at bit period (T_x) and the track pitch (T_z). Given here: A = 1 is amplitude of a 2-D pulse response, $w_x = W_x/2.5348$, $w_z = W_z/2.5348$, where W_x is an along-track PW50, and Wz is an cross-track PW50 repectively. As described by [6], the areal density of BPMR is limited by T_x and T_z according to the given below equation;

$$\text{Area density} = T_z/T_x \quad \text{bit/sq.inch} \tag{2}$$

BPMR channel with RS-LDPC concatenated code is illustrated in Fig. 1. A binary input sequence $a_{k,m} \in \{0,1\}$ is grouped to match the symbol size and encoded with a RS encoder. The output sequence $b_{k,m} \in \{0,1\}$ is subsequently encoded by a LDPC encoder. An RS encoder can be bypassed in the case that only LDPC code is required. Then the signal $u_{k,m} \in \{\pm 1\}$ is to be recorded into the media where $H_m(D)$ denotes the channel of the m-th track. The read back signal be written as

$$y_k = \sum_i \sum_m h_{i,m} u_{k-i,m} + n_k \tag{3}$$

Here hi_m's are the coefficient of 2-D channel response. D is an unit delay operator, and n_k is AWGN with zero mean and variance. In this system, we assume that the system has synchronized perfectly and the media characteristic is uniform without TMR effect. Target $G(D)$ and Equalizer $F(D)$ shown in Fig. 1 are generalized partial response targets (GPR) as described in [8].

Thebequalized sequence x_k is then fed to a turbo equalizer, which iteratively exchanges soft information between the SOVA equalizer and the LPDC decoder implemented based on a message passing algorithm with 3 internal iterations. A RS decoder is of neccessary just in the case of code concatenated scheme.

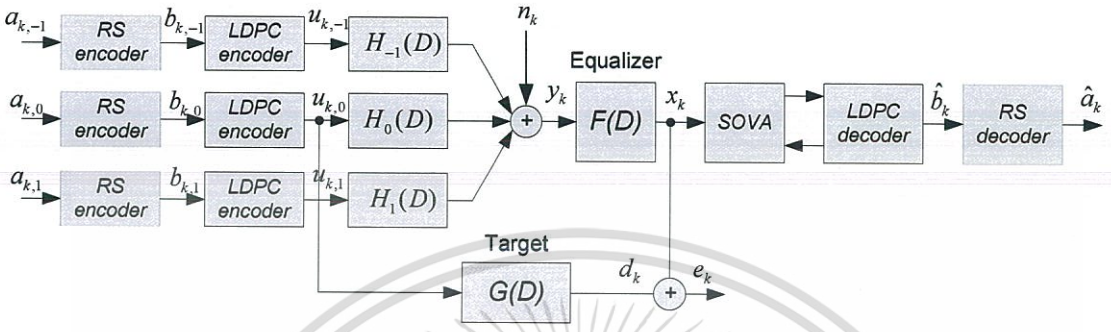


Fig. 1 A BPMR channel model with 1-D equalizer and 1-D target design

Error Correcting Code

Low Density Parity Check Code

LDPC codes are linear block codes which are define by a sparse parity check matrix, where the weights of the columns and the rows are far smaller than the size of its located columns and rows. The parity check matrix H of a QC-LDPC code can be constructed as given by (4) below.

$$H=\begin{bmatrix} I & I & I & \cdots & I & \cdots & I \\ 0 & I & \alpha^{1} & \cdots & \alpha^{j-2} & \cdots & \alpha^{k-2} \\ 0 & 0 & I & \cdots & \alpha^{2(j-2)} & \cdots & \alpha^{2(k-2)} \\ \vdots & \vdots & \vdots & & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & I & \cdots & \alpha^{(j-1)(k-1)} \end{bmatrix}_{pj\times pk} \tag{4}$$

Where $2 \le j \le k \le p$ and I is an identity matrix $(p\times p)$ and α is a position permuted matrix $(p\times p)$. An example of matrices I and α is given herewith in (5).

$$I=\begin{bmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \end{bmatrix}_{p\times p} \quad \alpha=\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & 0 & 0 & \cdots & 0 \end{bmatrix}_{p\times p} \tag{5}$$

For parity check matrix design, for the sake of simplicity, we employed the technique described in [9].

Reed Solomon Code

Reed-Solomon codes are non-binary cyclic codes with symbols made up of m-bit sequences, where m is any positive integer having a value greater than 2. R-S (n, k) codes on m-bit symbols exist for all n and k. Where k is the number of data symbols being encoded, and n is the total number of

code symbols in the encoded block. By adding $2t$ check symbols to the data, then an RS codes can detect any combination of error bits up to $2t$ erroneous symbols, or correct up to t symbols. The maximum codeword length (n) is $n=2^m-1$, where m is a symbol size.

Experiment Setup

From BPMR channel shown in Fig.1, we define areal density as 2Tb/in^2 and 2.5Tb/in^2 in equation (1) then the coefficients of a channel $H(D)$ can be computed as [6], [7]

$$H(D)_{2.5Tb/in^2} = \begin{bmatrix} 2.11\times10^{-4} & 0.0503 & 0.3124 & 0.0503 & 2.11\times10^{-4} \\ 1.08\times10^{-4} & 0.1612 & 1 & 0.1612 & 1.08\times10^{-4} \\ 2.11\times10^{-4} & 0.0503 & 0.3124 & 0.0503 & 2.11\times10^{-4} \end{bmatrix} \quad (6)$$

$$H(D)_{2Tb/in^2} = \begin{bmatrix} 2.54\times10^{-5} & 0.0238 & 0.2336 & 0.0238 & 2.54\times10^{-5} \\ 1.08\times10^{-4} & 0.1021 & 1 & 0.1021 & 1.08\times10^{-4} \\ 2.54\times10^{-5} & 0.0238 & 0.2336 & 0.0238 & 2.54\times10^{-5} \end{bmatrix} \quad (7)$$

The data in a sector is set to 4,075 bits. The target and equalize are defined similar in [7]. A block size of 3,586 bits is encoded with a LDPC encoder of an irregular (4, 25) with a code rate of 0.88. Similarly, a block size of 3423 bits is encoded with irregular (3, 25) LDPC encoder at a code rate of 0.84. For the concatenate coding scheme, we use an irregular (4, 25) LDPC code with a code rate of 0.88. It is combined with shortened RS code in $GF(2^9)$ with code rate of 0.95 and minimum distance is 10. As a result, the actual code rate is 0.84.

Simulation Results

Fig. 2 and Fig. 3 show the bit error rate and sector error rate performance of various codes; i.e. LDPC code with the rate of 0.88, rate of 0.84 and the concatenated code with the rate of 0.84. Obviously seen in BER:- LDPC with code rate of 0.84 is better than a concatenated code. Surprisingly when we look into SER, it is founded that the concatenated code is better. The LDPC code with rate of 0.88 is the most poorest compared to others

We all know that RS code cannot do anything if the number of errors excesses its capability (10 symbols, in this case). In such a situation, the presence of RS code has no meaning. However, the situation is improved if the number of errors is less than 10 symbols per block. This is why the SER can be made better.

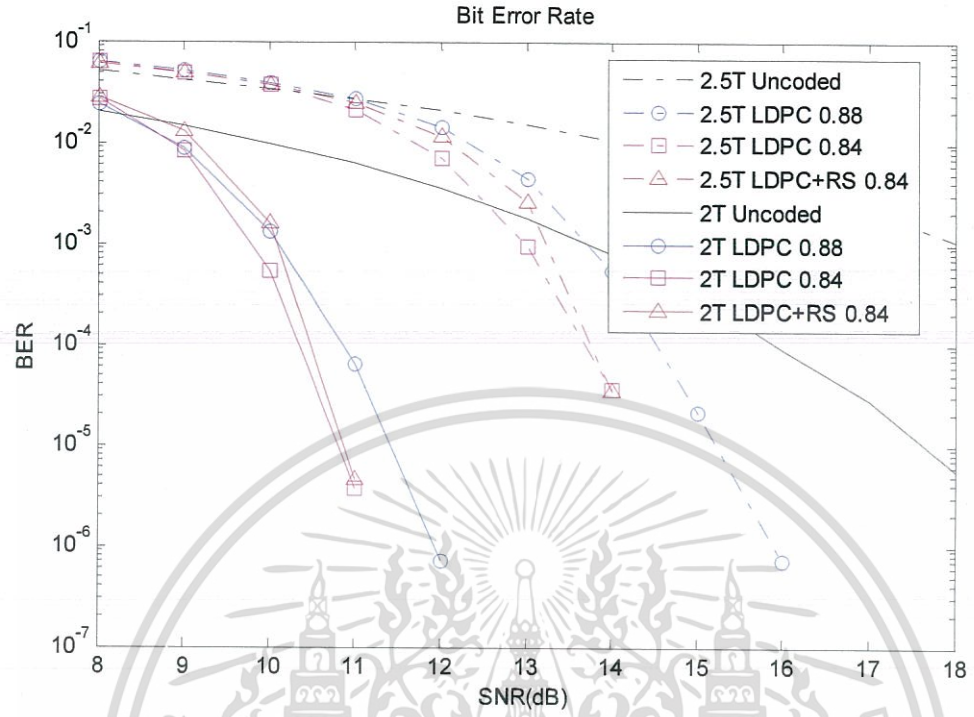


Fig. 2 Bit error rate performances

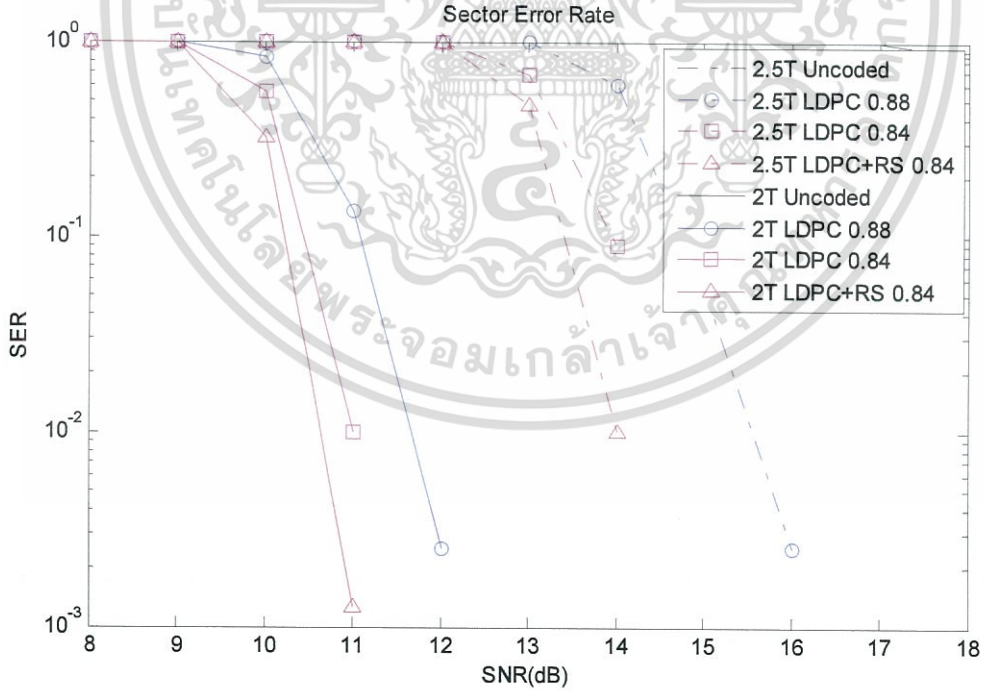


Fig. 3 Sector error rate performances

Conclusion

In this paper we have reported the performance evaluation of BPMR channel with and without concatenate code. By using the RS-LDPC concatenated code the sector error rate (SER) can be improved with a slight deteriorated in bit error rate (BER). SER can be the most desirable result since we can verify entire sector instead of number of error bits. Even though only single bit went wrong in same sector, the whole sector will be discarded. Therefore, the use of concatenated code in the ECC system with BPMR channel is superior compared to a conventional method that only RS code or LDPC code is used. Another bright side of the presence of RS code in the RS-LDPC concatenated code is that the burst error correcting can be made ideal. On the dim side, a concatenated code may require an additional processing step that can be a drawback for some implementation. This trade off should be considered case by case according to the actual requirement.

Acknowledgment

This work is partially supported by Industry/University Cooperative of Data Storage Technology and Applications Research Center (I/UCRC), King Mongkut's Institute of Technology Ladkrabang and National Electronic and Computer Technology Center (NECTEC), National Science and Technology Development Agency (NSTDA) under scholarship HDD-01-52-01D.

References

[1] S.X. Wang and A. M. Taratorin, Magnetics Information Technology. San Diego: Academic Press, 1999.

[2] J. M. Ruigrok, R. Coehoorn, S. R. Cumpson, and H. W. Kesteren, "Disk recoding beyond 100 Gb/in^2 : hybrid recoding?," *J. Applied Physics*, vol. 87, no. 9, pp. 5398 - 5403, May 2000.

[3] R. Wood, "The feasibility of magnetic recording at 1 terabit per square inch," *IEEE Trans. Magn.*, vol. 36, no. 1, pp. 36 - 42, January 2000.

[4] R. Wood, M. Williams, A. Kavcic, and J. Miles, "The feasibility of magnetic recording at 10 terabit per square inch on conventional media," *IEEE Trans. Magn.*, vol. 45, no. 2, pp. 917 - 923, February 2009.

[5] Thomas R. Albrecht, Daniel Bedau, Elizabeth Dobisz, He Gao, Michael Grobis, Olav Hellwig, Dan Kercher, Jeffrey Lille, Ernesto Marinero, Kanaiyalal Patel, Ricardo Ruiz, Manfred E. Schabes, Lei Wan, Dieter Weller, and Tsai-Wei Wu, "Bit Patterned Media at 1 Tdot/in and Beyond" *IEEE Trans. Magn.*, vol. 49, no. 2, pp. 773 - 778, February 2013.

[6] Nabavi S. Signal processing for bit-patterned media channel with inter-track interference. Ph.D. dissertation, Dept. Elect. Eng. Comp. Sci., Carnegie Mellon University, Pittsburgh, PA, 2008.

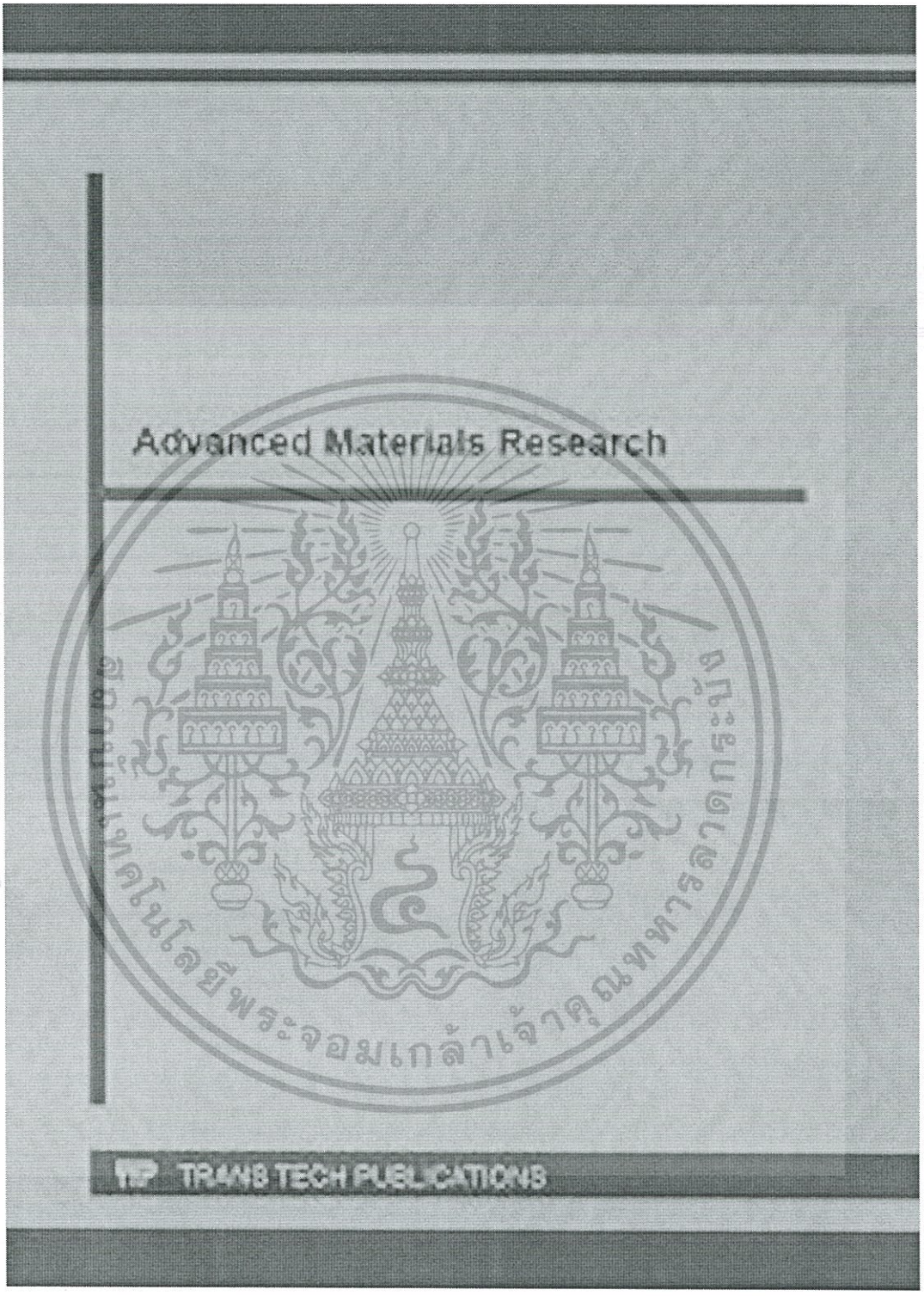
[7] S. Koonkarnkhaia, N. Chirdchoob, P. Kovintavewatb, "Iterative Decoding for High-Density Bit-Patterned Media" Procedia Engineering (32), pp.323-328, March 2012.

[8] Piya Kovintavewat, Inci Ozgunes, Erozan M. Kurtas, John R. Barry, and Steven W. McLaughlin, "Generalized partial response targets for perpendicular recording with jitter noise," *IEEE Trans. Magn.*, vol. 38, no. 5, pp. 2340 - 2342, September 2002.

[9] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello,Jr., "LDPC block and convolutional codes based on circulant matrices," IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 2966–2984, Dec. 2004.

Research in Materials and Manufacturing Technologies
10.4028/www.scientific.net/AMR.834-836

A Concatenate Code for Error Correcting Code in Bit Pattern Media Recoding System
10.4028/www.scientific.net/AMR.834-836.962



Advanced Materials Research Vol. 909 (2014) pp 338-341
Online available since 2014/Mar/24 at www.scientific.net

doi:10.4028/www.scientific.net/AMR.909.338

A Construction of Non Binary LDPC Codes by Circular Matrices

Sekson Timakul[1, a], Somsak Choomchuay[2,b]

[1]College of Data Storage Innovation, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand, Tel:/Fax: + 66-2-326-4731

[2]Faculty of Engineering, King Mongkut's Institute of Technology Ladkrabang, Bangkok 10520, Thailand Tel: +66-2-329-8344 Ext.114, Fax: +66-2-329-8346

[a]sekson.timakul@gmail.com, [b] kchsomsa@kmitl.ac.th

Keywords: Non-Binary LDPC, Error Correcting Code, GF(q), Parity Check Matrix.

Abstract. In LDPC code, the structure of code's parity check matrix plays the crucial role in code performance. In this paper proposes the preliminary investigation of a designed parity check matrix from Tanner. We modify this technique in to non binary LDPC structure and decoding with FFT-SPA. We take into high code rate application more than 0.8. The result has shown that in bit error rate (BER) compare between non-binary LDPC and binary LDPC. In our results, the performance of non binary LDPC has better than binary LDPC.

Introduction

Low Density Parity Check (LDPC) code was firstly invented by Gallager in 1962 [1]. This is a kind of linear block code which the parity checks matrix $\boldsymbol{H}$ has a low density of non-zero entries and these iterative decoding codes. The LDPC code has been widely adopted in area of error correcting code especially in digital communication such as WLAN and magnetic recording, etc. The LDPC codes over the Galois field of order q are non-binary LDPC (NB-LDPC) codes. This class of code was first investigated by Davey and MacKay in 1998 [2] and modify for reduce complexity decoder in fast Fourier transform by Barnaul and Declercq [3] and Song and Cruz [4]. There are many researches attend for various designs of parity check matrix. The most common use and high performance technique is Quasi-cyclic. This technique establishes by define the sub matrix in parity check matrix. The defined sub matrix called permutation matrix which is the identity matrix that the information bit was shifted to the right hand side. Based on circular permutation matrices, Tanner etc. [5], and Fossorier [6] proposed a design of parity check matrix by employed a class of algebraically structured quasi-cyclic. Timakul et al. [7] investigated Tanner method for parity check matrix $\boldsymbol{H}$ in binary LDPC for high code rate. Authors in [7] achieved bit error rate (BER) by 10^{-6} at signal to noise ratio (SNR) 4.5 dB by employing the binary LDPC decoding in AWGN channel.

This paper we propose an error correction coding scheme to correct the error in high rate application, and it is the extension of work in [7] by modifying a parity check matrix $\boldsymbol{H}$ for non binary LDPC. The sequence and modulo were defined elements in a circulant permutation matrices. The result is bit error rate (BER) by comparing the binary code and non binary LDPC. The rest of paper is organized as follows. We briefly introduce about decoding of non binary LDPC in next section II. The construction of parity check matrix for high code rate. In section III, we explain how the experimental is organized. In section IV, the performance outcome is shown. Finally, we conclude our achievement in section V.

The FFT for the Decoding of Non-Binary LDPC

A generalized sum-product algorithm (SPA) for decoding Q-ary LDPC codes called the Q-array SPA (QSPA) can reduce decoding complexity based on fast Fourier transforms (FFT). The combined procedure is also called FFT-QSPA. Although the FFT-QSPA reduces the computational complexity,

it has introduced another quite complicated operation such as permutation that relates to multiplications over GF(q). The FFT-SPA LDPC process is summarized in the following steps [8];

Initial Step: Quantities the probability of variable node: are initialized by f_n^x

Horizontal Step: Find the probability that parity check: which fast Fourier transforms

$$r_{mn}(x) = F^{-1}\left(\prod_{n' \in N_m / n} F(q_{mn'}(x))\right) \tag{1}$$

Vertical Step: Find the new probability of variable node: q_{mn}

$$q_{mn}(x) = \beta_{mn} f_n^x \prod_{m' \in M_n / m} r_{m'n}(x), \tag{2}$$

$$\beta_{mn} = \frac{1}{\sum_x f_n^x \cdot \prod_{m' \in M_n \setminus m} r_{m'n}(x)} \tag{3}$$

Tentative decoding: Find the new codeword: $\hat{c}_n$

$$\hat{c}_n = \arg\max_x \beta_n f_n^x \prod_{m \in N_n} r_{mn}(x). \tag{4}$$

Syndrome check:

$$H\hat{c} = 0 \tag{5}$$

If syndrome is zero, stop the decoding and get valid codeword, otherwise the algorithm repeats equation (1) to (5) until maximum number of iterations.

Construction of Non-Binary LDPC codes

In this section, we present a method for the parity check matrix H design. This structure can be represented by

$$H = \begin{bmatrix} P^{a} & P^{(a*b) \bmod p} & P^{(a*b^2) \bmod p} & \cdots & P^{(a*b^{j-1}) \bmod p} \\ P^{(a*c) \bmod p} & P^{(a*b*c) \bmod p} & P^{(a*b^2*c) \bmod p} & \cdots & P^{(a*b^{j-1}*c) \bmod p} \\ P^{(a*c^2) \bmod p} & P^{(a*b*c^2) \bmod p} & P^{(a*b^2*c^2) \bmod p} & \cdots & P^{(a*b^{j-1}*c^2) \bmod p} \\ \vdots & \vdots & \vdots & & \vdots \\ P^{(a*c^{k-1}) \bmod p} & P^{(a*b*c^{k-1}) \bmod p} & P^{(a*b^2*c^{k-1}) \bmod p} & \cdots & P^{(a*b^{j-1}*c^{k-1}) \bmod p} \end{bmatrix}_{pj \times pk} \tag{6}$$

$$P^1 = \begin{bmatrix} 0 & \alpha_1 & 0 & \dots & 0 & 0 & 0 \\ 0 & 0 & \alpha_2 & \dots & 0 & 0 & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & \alpha_{p-2} & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & \alpha_{p-1} \\ \alpha_p & 0 & 0 & \vdots & 0 & 0 & 0 \end{bmatrix}_{p \times p} \quad (7)$$

The number a, b and c in equation (6) are bounded within modulo permutation size p. Let GF(q) be a finite field with q elements. We define α in equation (7) are non-zero elements in GF(q) while $\alpha \in \{1,\dots,q-1\}$.

Experiment

To evaluate the effectiveness on the design of parity check matrix, we employed AWGN as reference channel model. The performance will be compared between binary LDPC which designed by [5] and non-binary LDPC over GF(256). The variable parameters for evaluation are defined in Table I.

Table 1. The design parameter

Type	Galois filed	Row weigh (d_v)	Column weigh (d_c)	Code rate	Maximum iteration	Code length (bits)
Binary LDPC	GF(2)	4	40	0.9	20	4,120
Non-binary LDPC	GF(256)	2	18	0.8888	20	4,176

Simulation Results

The obtained result is shown in figure 1 where the bit error rate (BER) performance is illustrated. In figure 1, the performance of non binary LDPC provides better binary LDPC performance.

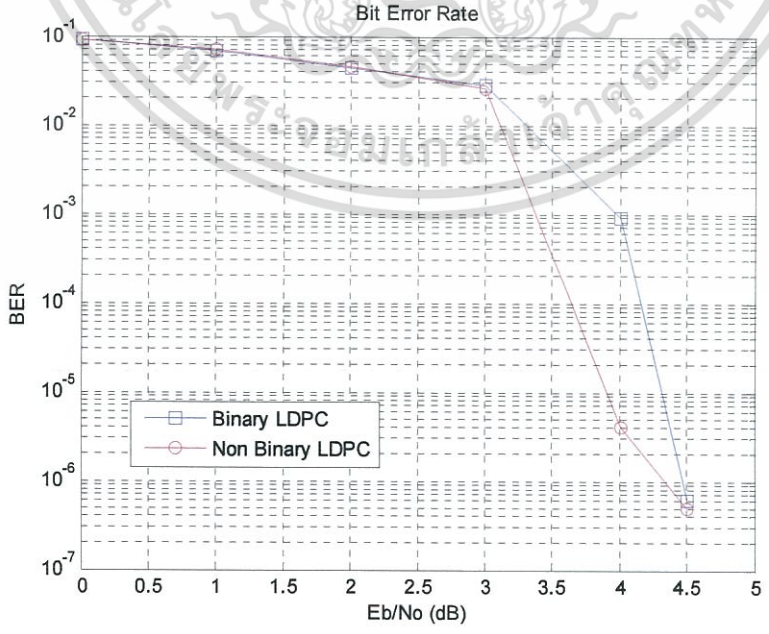


Fig. 1 Bit error rate performance

Conclusion

In this paper we have proposed a parity check matrix $\boldsymbol{H}$ design of a non binary LDPC code. The method modified technique cyclic shifting from binary LDPC. The main task is to design the first row sub-matrices. The subsequent rows are basically the shifted version of the previous row. This method can ensure the absence of cycle-4. From the experiment at high code rate, our proposed scheme by employing non binary ldpc with GF(256) can achieve performance better than binary LDPC. This cause of non binary decoding employed symbol correction whereas the binary LDPC using bit instead.

Acknowledgment

This work is partially supported by Industry/University Cooperative of Data Storage Technology and Applications Research Center (I/UCRC), King Mongkut's Institute of Technology Ladkrabang and National Electronic and Computer Technology Center (NECTEC), National Science and Technology Development Agency (NSTDA) under scholarship HDD-01-52-05D.

References

[1] R. G. Gallager, "Low-density parity-check codes," Ph.D. dissertation, Department of Electrical Engineering, M.I.T., Cambridge, Mass., July 1963.

[2] M. Davey and D. MacKay, "Low density parity check codes over GF (q)," Information Theory Workshop, 1998, pp. 70-71, 1998.

[3] L. Barnault and D. Declercq, "Fast Decoding Algorithm for LDPC over GF (2q)," The Proc. 2003 Inform.Theory Workshop, pp. 70–73, 2003.

[4] H. Song and J. R. Cruz, "Reduced-complexity decoding of q-ary LDPC codes for magnetic recording," IEEE Trans. Magn., vol. 39, no. 2, pp. 1081–1087, 2003.

[5] R. M. Tanner, D. Sridhara, A. Sridharan, T. E. Fuja, and D. J. Costello,Jr., "LDPC block and convolutional codes based on circulant matrices," IEEE Trans. Inform. Theory, vol. 50, no. 12, pp. 2966-2984, 2004.

[6] M. P. C. Fossorier, "Quasi-cyclic low-density parity-check codes from circulant permutation matrices," IEEE Trans. Inform Theory, vol. 50, no. 8, pp. 1788-1793, 2004.

[7] S. Timakul and S. Choomchuay, "Construction of quasi-cyclic LDPC codes form SFT structure and cyclic shift," Intelligent Signal Processing and Communications Systems (ISPACS), pp. 1081–1087, 2011.

[8] Rolando Antonio Carrasco and Martin Johnston, "Non-Binary Error Control Coding For Wireless Communication And Data Storage", John Willey & Sons, Ltd., pp. 201-235, 2008.

Manufacturing and Applied Research
10.4028/www.scientific.net/AMR.909

A Construction of Non Binary LDPC Codes by Circular Matrices
10.4028/www.scientific.net/AMR.909.338

ประวัติผู้เขียน

ชื่อ-นามสกุล	นาย เสกสรรค์ ธิมากุล	
ที่อยู่	28 หมู่ที่ 1 ตำบลท่าหลวง อำเภอท่าเรือ จังหวัดพระนครศรีอยุธยา	
อีเมล์	sekson.timakul@gmail.com	

ประวัติการศึกษา	2548	วิศวกรรมศาสตร์มหาบัณฑิต สาขาวิชาวิศวกรรมไมโครอิเลคทรอนิคส์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
	2545	วิศวกรรมศาสตร์บัณฑิต สาขาวิชาวิศวกรรมอิเลคทรอนิคส์ สถาบันเทคโนโลยีพระจอมเกล้าเจ้าคุณทหารลาดกระบัง
	2540	ประกาศนียบัตรวิชาชีพชั้นสูง สาขาวิชาช่างอิเลคทรอนิคส์ วิทยาลัยเทคนิคราชสิทธาราม
	2538	ประกาศนียบัตรวิชาชีพ สาขาวิชาช่างอิเลคทรอนิคส์ วิทยาลัยเทคนิคราชสิทธาราม
ประสบการณ์การทำงานและผลงานวิจัย	2548-2551	วิศวกรบริษัท เวสเทิร์น ดิจิตอล (ประเทศไทย) จำกัด
	2545-2546	ผู้ช่วยนักวิจัยศูนย์วิจัยอิเลคทรอนิคส์ (ERC) ในโครงการสร้างวงจรซีมอสเทคโนโลยี 5 ไมครอนในประเทศไทย